GUIDE D'ADMINISTRATION

Cisco Small Business

RV110W Pare-feu VPN Wireless-N

Révisé mars 2012

Cisco et le logo Cisco sont des marques commerciales ou des marques commerciales déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales de Cisco, rendez-vous sur : **www.cisco.com/go/trademarks**. Les autres marques de commerce mentionnées sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et une autre société. (1110R)

© 2011-2012 Cisco Systems, Inc. Tous droits réservés.

78-20157-03 (précédemment OL-21745-01)

Table des matières

Chapitre 1 : Introduction 9

Présentation du produit 9
Présentation du routeur Cisco RV110W 11
Panneau avant 11
Panneau arrière 12
Installation du Cisco RV110W 14
Choix de l'emplacement 14
Connexion de l'équipement 14
Utilisation de l'assistant de configuration 17
Utilisation de la page Mise en route 18

Chapitre 1 : Mise en route 18

Navigation dans les pages 20
Enregistrement des modifications 21
Affichage des fichiers d'aide 21
Étapes suivantes de la configuration 22
Vérification de l'installation matérielle 22
Connexion au réseau sans fil 23

Chapitre 2 : Configuration du réseau 24

Configuration des paramètres WAN 25
Configuration de la configuration automatique (DHCP) 25
Configuration d'une adresse IP statique 25
Configuration du protocole PPPoE 26
Configuration du protocole PPTP 27
Configuration du protocole L2TP 29
Configurer les paramètres facultatifs 31
Configuration des paramètres LAN 32
Modification de l'adresse IP par défaut du Cisco RV110W 32
Configuration de DHCP 33
Configuration des VLAN 35

Configuration de DHCP statique 36
Affichage des baux de clients DHCP 37
Configuration d'un hôte de DMZ 38
Configuration de RSTP 39
Gestion des ports 40
Clonage de l'adresse MAC 42
Configuration du routage 43
Configuration du mode de fonctionnement 43
Configuration du routage dynamique 44
Configuration du routage statique 45
Configurer le routage inter VLAN 46
Affichage de la table de routage 46
Configuration du DNS dynamique 46
Configuration du mode IP 48
Configuration d'IPv6 49
Configuration du WAN pour un réseau IPv6 49
Configuration des paramètres LAN IPv6 53
Configurer le routage IPv6 statique 55
Configuration du routage (RIPng) 57
Configuration du tunneling 58
Affichage de l'état du tunnel IPv6 59
Configuration de l'annonce du routeur 59
Configuration des préfixes d'annonce 61

Chapitre 3 : Configuration du réseau sans fil 63

Sécurité sans fil 63
Conseils relatifs à la sécurité des réseaux sans fil 63
Directives générales sur la sécurité réseau 65
Réseaux sans fil Cisco RV110W 65
Configuration des paramètres sans fil de base 66
Modification des paramètres de réseau sans fil 68

Configurer le mode de sécurité 69
Configuration du filtrage MAC 73
Configuration de l'accès par horaire 74
Configuration du réseau invité sans fil 74
Configuration des paramètres sans fil avancés 76
Configuration de WDS 80
Configuration de WPS 81

Chapitre 4 : Configuration du pare-feu 83

Fonctionnalités de pare-feu du Cisco RV110W 83
Configuration des paramètres de base du pare-feu 85
Configuration de la gestion à distance 88
Configuration d'Universal Plug and Play 89
Gestion des horaires de pare-feu 89
Ajout ou modification d'un horaire de pare-feu 89
Configuration de la gestion de services 90
Configuration des règles d’accès 91
Ajout de règles d'accès 92
Création d'une stratégie d'accès à Internet 95
Ajout ou modification d'une stratégie d'accès à Internet 95
Configuration de la redirection de ports 97
Configuration de la redirection de port individuel 97
Configuration de la redirection d'une plage de ports 98
Configuration du déclenchement de plage de ports 98

Chapitre 5 : Configuration de VPN 100

Types de tunnels VPN 100
Clients VPN 101
Configuration du protocole PPTP 102
Configuration de NetBIOS sur VPN 103
Création et gestion des utilisateurs PPTP 103

Création et gestion des utilisateurs QuickVPN 104
Importation des paramètres client VPN 104
Configuration des paramètres VPN de base (VPN site-à-site) 105
Affichage des valeurs par défaut 107
Configuration des paramètres VPN avancés 107
Gestion des stratégies IKE 107
Gestion des stratégies VPN 108
Configuration de la gestion des certificats 113
Configuration de l'intercommunication VPN 115

Chapitre 6 : Configuration de la Qualité de service (QoS) 116

Configuration de la gestion de la bande passante 116
Configuration de la bande passante 116
Configuration des priorités de bande passante 117
Configuration des paramètres de port QoS 118
Configuration des paramètres CoS 119
Configuration des paramètres DSCP 120

Chapitre 7 : Administration de votre Cisco RV110W 121

Définition de la complexité des mots de passe 122
Configuration des comptes d'utilisateurs 123
Définition du délai d'expiration de session 124
Configuration SNMP (Simple Network Management Protocol) 124
Configuration des informations système SNMP 125
Modification des utilisateurs SNMPv3 126
Configuration des filtres SNMP 127
Utilisation des outils de diagnostic 127
Outils réseau 128
Configuration de la mise en miroir des ports 129
Configuration de la journalisation 130
Configuration des paramètres de journalisation 130

Configuration de l'envoi des journaux par e-mail 132
Configuration de Bonjour 134
Configuration des paramètres de date et d'heure 135
Sauvegarde et restauration du système 136
Sauvegarde des paramètres de configuration 137
Restauration des paramètres de configuration 138
Copie des paramètres de configuration 138
Génération d'une clé de chiffrement 139
Mise à niveau du micrologiciel ou modification de la langue 139
Redémarrage du Cisco RV110W 141
Restauration des paramètres d'usine 141
Exécution de l'assistant de configuration 141

Chapitre 8 : Affichage de l'état du Cisco RV110W 142

Affichage du tableau de bord 143
Affichage du récapitulatif du système 145
Affichage des statistiques relatives au réseau sans fil 148
Affichage de l'état du VPN 149
Affichage de l'état des connexions IPsec 150
Affichage des journaux 151
Affichage des périphériques connectés 152
Affichage des statistiques des ports 153
Affichage de l'état du réseau invité 154

Annexe A : Utilisation de Cisco QuickVPN 155

Présentation 155
Avant de commencer 155
Installation du logiciel Cisco QuickVPN 156
Installation à partir du CD-ROM 156
Téléchargement et installation à partir d'Internet 158

Utilisation du logiciel Cisco QuickVPN 158

Annexe B : Pour en savoir plus 162

1

Introduction

Ce chapitre fournit des informations qui vous permettent de vous familiariser avec les caractéristiques du produit, qui vous guident tout au long du processus d'installation et vous permettent de commencer à utiliser le gestionnaire de dispositifs basé sur navigateur.

- **Présentation du produit**
- **Présentation du routeur Cisco RV110W**
- **Installation du Cisco RV110W**
- **Connexion de l'équipement**
- **Utilisation de l'assistant de configuration**
- **Vérification de l'installation matérielle**
- **Connexion au réseau sans fil**

Présentation du produit

Merci d'avoir choisi le pare-feu VPN Wireless-N RV110W Cisco Small Business.

Le Cisco RV110W est une solution réseau de partage Internet avancée répondant aux besoins des petites entreprises. Il permet de partager une connexion Internet entre plusieurs ordinateurs de votre bureau par le biais de connexions câblées et sans fil.

Le Cisco RV110W fournit un point d'accès Wireless-N associé à la prise en charge de clients VPN (réseau privé virtuel), renforçant la sécurité des accès distants à votre réseau.

L'interface 10/100 Fast Ethernet WAN du routeur se connecte directement à votre modem haut débit DSL ou modem câble.

Interfaces LAN Ethernet

Le Cisco RV110W présente quatre interfaces LAN 10/100 Fast Ethernet en duplex intégral permettant de connecter jusqu'à quatre périphériques. Vous pouvez connecter un commutateur Cisco Small Business à l'un des ports disponibles pour étendre votre réseau selon les besoins.

Point d'accès sans fil

Le point d'accès sans fil du Cisco RV110W prend en charge la norme 802.11n avec la technologie MIMO, multipliant ainsi le débit de données effectif. Cette technologie engendre un débit et une couverture supérieurs à ceux qu'offrent les réseaux 802.11g.

Accès au pare-feu et aux clients VPN

Le routeur Cisco RV110W intègre un pare-feu à filtrage dynamique des paquets (SPI) avec prévention des dénis de service (DoS) et un moteur VPN pour garantir la sécurité des communications entre les employés mobiles ou distants et les succursales.

Le Cisco RV110W prend en charge jusqu'à cinq tunnels VPN client-passerelle pour faciliter la connectivité avec les filiales via des liens virtuels cryptés. Les utilisateurs se connectant par le biais d'un tunnel VPN sont rattachés au réseau de votre société avec un accès sécurisé aux fichiers, au courrier électronique et à votre intranet, comme s'ils étaient dans vos locaux.

Sécurité

Le Cisco RV110W met en œuvre les protections WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise et WEP aux côtés d'autres fonctions de sécurité telles que la désactivation des diffusions SSID, le filtrage basé sur MAC et l'autorisation ou l'interdiction des accès par horaire pour chaque SSID.

Qualité de service

Le Cisco RV110W prend en charge les spécifications Wi-Fi Multimedia (WMM) et Wi-Fi Multimedia Power Save (WMM-PS) pour la qualité de service (QoS).

Le Cisco RV110W prend également en charge 802.1p, Differentiated Services Code Point (DSCP) et Type de service (ToS) pour la QoS câblée, ce qui peut améliorer la qualité du réseau en cas d'utilisation d'applications sensibles aux retards, telles que la VoIP (voix sur IP), ou gourmandes en bande passante, telles que la lecture vidéo en continu.

Système de distribution sans fil

Le point d'accès sans fil du Cisco RV110W prend en charge le système de distribution sans fil WDS (Wireless Distribution System), qui permet d'étendre la couverture sans fil, sans ajout de câbles.

Réseaux virtuels

Le Cisco RV110W prend également en charge plusieurs SSID (Service Set Identifier) pour l'utilisation de réseaux virtuels (jusqu'à quatre réseaux virtuels distincts), avec la prise en charge VLAN basée sur 802.1Q pour la séparation du trafic.

Configuration et administration

Le serveur Web intégré du Cisco RV110W permet de configurer les paramètres du Cisco RV110W à l'aide du gestionnaire de dispositifs basé sur navigateur. Le Cisco RV110W prend en charge les navigateurs Web Internet Explorer, Firefox et Safari.

Le Cisco RV110W propose également un assistant de configuration qui permet de configurer facilement et rapidement les paramètres de base du Cisco RV110W.

Présentation du routeur Cisco RV110W

Panneau avant

	Alimentation	Le voyant d'alimentation devient vert lorsque l'unité est sous tension. Le voyant vert clignote au moment de la mise sous tension.
	WPS	Le bouton WPS (accès Wi-Fi protégé) permet de configurer l'accès sans fil pour les périphériques compatibles WPS de votre réseau. Pour plus d'informations, reportez-vous à la section **Configuration de WPS, page 81**.
	WAN	Le voyant WAN (Internet) s'allume en vert lorsque le Cisco RV110W est connecté à Internet via le modem câble ou DSL. Le voyant s'éteint lorsque le Cisco RV110W n'est pas connecté à Internet. Le voyant clignote en vert lors de l'envoi ou de la réception de données.
	Voyant WIRELESS	Le voyant sans fil est vert lorsque le module sans fil est activé. Le voyant s'éteint lorsque le module sans fil est désactivé. Le voyant clignote en vert lorsque le pare-feu envoie ou reçoit des données via le module sans fil.
	Ports LAN	Les voyants numérotés correspondent aux ports LAN sur le Cisco RV110W. Si les voyants restent allumés en vert en continu, l'unité Cisco RV110W est connectée à un périphérique via le port correspondant (1, 2, 3 ou 4). Le voyant d'un port clignote en vert lorsque le pare-feu envoie ou reçoit des données via ce port.

Panneau arrière

Bouton RESET (Réinitialisation)	Si le Cisco RV110W n'arrive pas à se connecter à Internet, appuyez sur le bouton **RESET** pendant au moins 3 secondes, mais pas plus de 10 secondes, à l'aide d'un trombone ou d'un objet similaire. Vous obtenez le même effet que lorsque vous appuyez sur le bouton de réinitialisation de votre ordinateur pour le redémarrer. Si vous rencontrez de graves problèmes avec le Cisco RV110W et que vous avez essayé toutes les autres mesures de dépannage, appuyez et maintenez enfoncé le bouton **RESET** pendant plus de 10 secondes. Ceci redémarre l'unité et restaure les valeurs par défaut. Les modifications apportées précédemment aux paramètres du Cisco RV110W sont alors perdues.
Ports LAN (1–4)	Connexions LAN aux périphériques réseau, tels que ordinateurs, serveurs d'impression ou commutateurs.
WAN	Le port WAN (Internet) est connecté à votre périphérique Internet, tel qu'un modem câble ou DSL.
Bouton POWER (Alimentation)	Appuyez sur cette touche pour activer ou désactiver le Cisco RV110W.
Port 12VDC	Connectez l'adaptateur secteur 12V AC fourni au port 12VDC.

Installation du Cisco RV110W

Choix de l'emplacement

- **Température ambiante** : pour éviter toute surchauffe du pare-feu, ne l'installez pas dans une zone où la température ambiante est supérieure à 40 °C.
- **Ventilation** : vérifiez que la ventilation est suffisante autour du pare-feu.
- **Charge mécanique** : le pare-feu doit être horizontal et stable pour éviter toute situation dangereuse.

Placez le Cisco RV110W à l'horizontale sur une surface plane afin que les pieds en caoutchouc soient en contact avec cette dernière.

Connexion de l'équipement

Connectez un ordinateur à un câble Ethernet pour effectuer la configuration initiale. Après avoir effectué cette configuration, vous pouvez exécuter les tâches d'administration en utilisant une connexion sans fil.

ÉTAPE 1 Mettez tous les appareils hors tension, y compris le modem câble ou DSL, l'ordinateur et le Cisco RV110W.

ÉTAPE 2 Un câble Ethernet doit déjà être utilisé pour la connexion de votre ordinateur au modem câble ou DSL. Débranchez une extrémité du câble de votre ordinateur et branchez-la sur le port WAN de l'unité.

ÉTAPE 3 Branchez l'extrémité d'un autre câble réseau Ethernet à l'un des ports LAN (Ethernet) numérotés à l'arrière de l'unité. (Dans cet exemple, le port LAN 1 est utilisé.) Connectez l'autre extrémité à un port Ethernet sur l'ordinateur que vous utiliserez pour exécuter le gestionnaire de dispositifs et l'assistant de configuration Web.

ÉTAPE 4 Mettez le modem câble ou DSL sous tension et attendez que la connexion soit active.

ÉTAPE 5 Connectez l'adaptateur secteur au port d'alimentation (12VDC) du Cisco RV110W.

ATTENTION Utilisez uniquement l'adaptateur secteur fourni avec l'unité. L'utilisation d'un autre adaptateur secteur pourrait endommager l'unité.

ÉTAPE 6 Branchez l'autre extrémité de l'adaptateur sur une prise secteur. Il est possible que vous ayez besoin d'utiliser une fiche spécifique (fournie) pour votre pays.

ÉTAPE 7 Sur le Cisco RV110W, enfoncez le bouton **POWER** pour mettre le pare-feu sous tension.

Le voyant d'alimentation situé sur le panneau avant est vert lorsque l'adaptateur secteur est correctement branché et que l'unité fonctionne.

Utilisation de l'assistant de configuration

L'assistant de configuration et le gestionnaire de dispositifs sont pris en charge sur Microsoft Internet Explorer 6.0 ou version ultérieure, Mozilla Firefox 3.0 ou version ultérieure et Apple Safari 3.0 ou version ultérieure.

Pour utiliser l'assistant de configuration :

ÉTAPE 1 Démarrez l'ordinateur que vous avez connecté au port LAN1 à l'étape 2 de la section **Connexion de l'équipement**.

L'ordinateur devient un client DHCP du Cisco RV110W et reçoit une adresse IP dans la plage 192.168.1.xxx.

ÉTAPE 2 Ouvrez une page Web et saisissez **192.168.1.1** dans la barre d'adresse. Il s'agit de l'adresse IP par défaut du Cisco RV110W.

Un message s'affiche concernant le certificat de sécurité du site. Le Cisco RV110W utilise un certificat de sécurité auto-signé et ce message s'affiche parce que l'ordinateur ne reconnaît pas le Cisco RV110W.

ÉTAPE 3 Cliquez sur **Poursuivre sur ce site Web** (ou l'option affichée sur votre navigateur Web spécifique) pour accéder au site Web.

ÉTAPE 4 Lorsque la page d'ouverture de session s'affiche, saisissez votre nom d'utilisateur et votre mot de passe.

Le nom d'utilisateur par défaut est **cisco**. Le mot de passe par défaut est **cisco**. Les mots de passe sont sensibles à la casse.

ÉTAPE 5 Cliquez sur **Se connecter**. L'assistant de configuration démarre.

ÉTAPE 6 Suivez les instructions affichées à l'écran pour configurer le Cisco RV110W.

L'assistant de configuration tente de détecter et de configurer automatiquement votre connexion. S'il n'y parvient pas, l'assistant de configuration peut vous inviter à fournir certaines informations sur votre connexion Internet. Il vous faudra peut-être contacter votre fournisseur de services Internet (FAI) pour obtenir ces informations.

REMARQUE : lors de l'utilisation de l'assistant de configuration, vous ne pouvez configurer qu'un seul réseau sans fil, ou SSID. Le Cisco RV110W prend en charge jusqu'à quatre réseaux sans fil. Si vous souhaitez configurer des réseaux sans fil supplémentaires, utilisez le gestionnaire de dispositifs Web. Reportez-vous à la section **Configuration du réseau sans fil**.

Une fois la configuration du Cisco RV110W par l'assistant de configuration terminée, vous devez modifier le mot de passe par défaut. Nous vous recommandons de tenir compte des règles de complexité des mots de passe ; voir la section **Définition de la complexité des mots de passe**.

Après avoir changé le mot de passe par défaut, la page **Mise en route** s'affiche. Pour plus d'informations, reportez-vous à la section **Utilisation de la page Mise en route**.

Utilisation de la page Mise en route

Mise en route

La page **Mise en route** affiche les tâches de configuration du Cisco RV110W les plus courantes. Utilisez les liens de cette page pour passer directement à la page de configuration pertinente.

Par défaut, cette page s'affiche au démarrage du gestionnaire de dispositifs. Toutefois, vous pouvez modifier ce comportement en cochant la case **Ne pas afficher au démarrage**, située au bas de la page.

Paramètres d'origine

Modifier le mot de passe d'administrateur par défaut	Cliquez sur ce lien pour ouvrir la page **Utilisateurs**, où vous pouvez modifier le mot de passe administrateur. Reportez-vous à la section **Configuration des comptes d'utilisateurs**.
Lancer l'assistant de configuration	Cliquez sur ce lien pour lancer l'assistant de configuration.

Configurer les paramètres WAN	Cliquez sur ce lien pour ouvrir la page **Configuration Internet**. Reportez-vous à la section **Configuration des paramètres WAN**.
Configurer les paramètres LAN	Cliquez sur ce lien pour ouvrir la page **Configuration LAN**. Reportez-vous à la section **Configuration des paramètres LAN**.
Configurer les paramètres sans fil	Cliquez sur ce lien pour ouvrir la page **Paramètres de base**. Reportez-vous à la section **Configuration des paramètres sans fil de base**.

Accès rapide

Mettre à niveau le micrologiciel du routeur	Cliquez sur ce lien pour ouvrir la page **Mise à niveau du micrologiciel/de la langue**. Reportez-vous à la section **Mise à niveau du micrologiciel ou modification de la langue**.
Ajouter des clients VPN	Cliquez sur ce lien pour ouvrir la page **Clients VPN**. Reportez-vous à la section **Clients VPN**.
Configurer l'accès pour la gestion à distance	Cliquez sur ce lien pour ouvrir la page **Paramètres de base**. Reportez-vous à la section **Configuration des paramètres de base du pare-feu**.

État de l'appareil

Récapitulatif du système	Cliquez sur ce lien pour ouvrir la page **Récapitulatif du système**. Reportez-vous à la section **Affichage du récapitulatif du système**.
État du réseau sans fil	Cliquez sur ce lien pour ouvrir la page **Statistiques sans fil**. Reportez-vous à la section **Affichage des statistiques relatives au réseau sans fil**.
État du VPN	Cliquez sur ce lien pour ouvrir la page **Clients VPN**. Reportez-vous à la section **Affichage de l'état du VPN**.

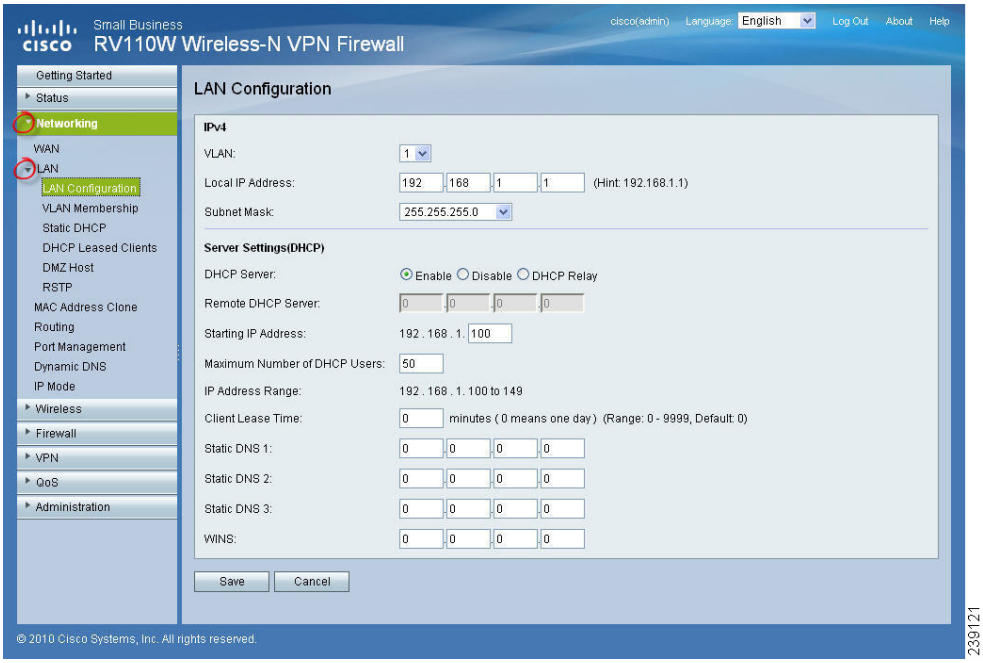
Autres ressources

Assistance	Cliquez sur ce lien pour ouvrir la page d'assistance Cisco.
Forums	Cliquez sur ce lien pour visiter les forums d'assistance en ligne de Cisco.

Navigation dans les pages

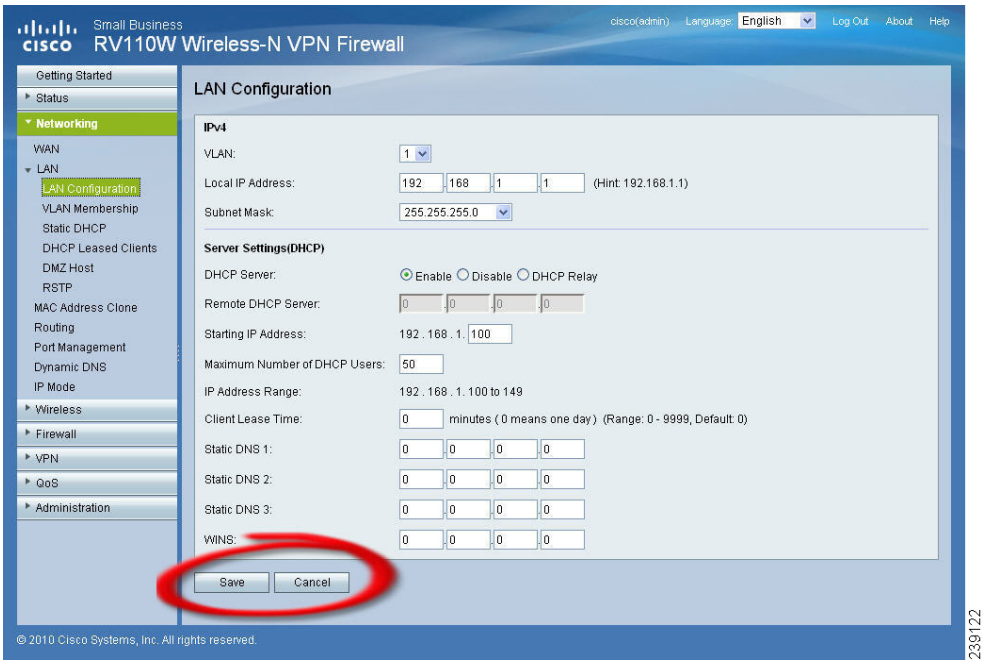
Utilisez l'arborescence du volet de gauche pour ouvrir les pages de configuration.

Cliquez sur les options de menu du volet gauche pour les développer. Cliquez sur un nom de menu affiché en dessous pour exécuter une action ou afficher un sous-menu.



Enregistrement des modifications

Après avoir terminé les modifications dans une page de configuration, cliquez sur **Enregistrer** pour enregistrer les modifications ou sur **Annuler** pour les annuler.



Affichage des fichiers d'aide

Pour afficher davantage d'informations sur une page de configuration, cliquez sur le lien **Aide** situé dans l'angle supérieur droit de la page.

Étapes suivantes de la configuration

Bien que l'assistant de configuration configure automatiquement le Cisco RV110W, il est recommandé de modifier certains des paramètres par défaut pour renforcer la sécurité et les performances.

Vous pouvez en outre être amené à configurer manuellement certains paramètres. Les étapes recommandées sont décrites ci-après :

1. Modifiez la valeur d'expiration après inactivité qui est de 10 minutes par défaut gestionnaire de dispositifs. Cela peut être gênant si vous êtes en train d'essayer de configurer votre périphérique. Reportez-vous à la section **Définition du délai d'expiration de session**.
2. (Facultatif) Si vous utilisez déjà un serveur DHCP sur votre réseau et si vous ne souhaitez pas que le Cisco RV110W fasse office de serveur DHCP, reportez-vous à **Configuration des paramètres LAN**.
3. Configurez votre réseau sans fil, en particulier la sécurité sans fil. Reportez-vous à la section **Chapitre 3, « Configuration du réseau sans fil »**.
4. Configurez votre réseau privé virtuel (VPN) à l'aide de QuickVPN. Le logiciel QuickVPN se trouve sur le CD de documentation et du logiciel fourni avec le pare-feu. Reportez-vous à l'**Annexe A, «Utilisation de Cisco QuickVPN»**.

Vérification de l'installation matérielle

Pour vérifier l'installation matérielle, procédez comme suit :

- Vérifiez l'état des voyants LED. Ils sont décrits dans la section **Présentation du routeur Cisco RV110W**.
- Connectez un ordinateur à un port LAN libre et vérifiez que vous pouvez vous connecter à un site Web sur Internet, par exemple www.cisco.com.
- Configurez un périphérique pour le connecter au réseau sans fil et assurez-vous que le réseau sans fil fonctionne. Reportez-vous à la section **Connexion au réseau sans fil**.

Connexion au réseau sans fil

Pour connecter un périphérique (tel qu'un ordinateur) à votre réseau sans fil, vous devez configurer la connexion sans fil sur le périphérique avec les informations de sécurité sans fil que vous avez configurées pour le Cisco RV110W à l'aide de l'assistant de configuration.

Les étapes suivantes sont indiquées à titre d'exemple ; vous pouvez choisir une autre configuration pour votre périphérique. Pour les instructions relatives à votre périphérique, consultez la documentation correspondante.

ÉTAPE 1 Ouvrez la fenêtre ou le programme de paramétrage de la connexion sans fil de votre périphérique.

Votre ordinateur peut comporter un logiciel spécial pour gérer les connexions sans fil. Vous pouvez également afficher les connexions sans fil dans la fenêtre **Connexions réseau** ou **Réseau et Internet** du Panneau de configuration. (L'emplacement varie selon le système d'exploitation.)

ÉTAPE 2 Saisissez le nom de réseau (SSID) choisi pour votre réseau dans l'assistant de configuration.

ÉTAPE 3 Choisissez le type de chiffrement et saisissez la clé de sécurité que vous avez spécifiée dans l'assistant de configuration.

Si vous n'avez pas activé la sécurité (déconseillé), ne renseignez pas les champs de chiffrement sans fil configurés avec le type de sécurité et le mot de passe.

ÉTAPE 4 Vérifiez votre connexion sans fil et enregistrez vos paramètres.

2

Configuration du réseau

Ce chapitre indique la marche à suivre pour configurer les paramètres réseau du Cisco RV110W.

- **Configuration des paramètres WAN**
- **Configuration des paramètres LAN**
- **Clonage de l'adresse MAC**
- **Configuration du routage**
- **Gestion des ports**
- **Configuration du DNS dynamique**
- **Configuration du mode IP**
- **Configuration d'IPv6**

Configuration des paramètres WAN

La configuration des propriétés WAN d'un réseau IPv4 dépend du type de connexion Internet que vous utilisez.

Configuration de la configuration automatique (DHCP)

Configuration de la configuration automatique (DHCP)

Si votre fournisseur d'accès à Internet (FAI) utilise la norme DHCP (Dynamic Host Control Protocol) pour vous affecter une adresse IP, vous recevez une adresse IP dynamique générée à chaque fois que vous vous connectez.

Pour configurer les paramètres WAN DHCP :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **WAN**.

ÉTAPE 2 Dans le menu déroulant **Type de connexion Internet**, sélectionnez **Configuration automatique - DHCP**.

ÉTAPE 3 (Facultatif) Pour configurer les paramètres facultatifs, voir la section **Configurer les paramètres facultatifs**.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration d'une adresse IP statique

Configuration d'une adresse IP statique

Si votre FAI vous a affecté une adresse IP permanente, effectuez les opérations suivantes pour configurer vos paramètres WAN :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **WAN**.

ÉTAPE 2 Dans le menu déroulant **Type de connexion Internet**, sélectionnez **IP statique**.

ÉTAPE 3 Saisissez les informations suivantes :

Adresse IP Internet	Entrez l'adresse IP du port WAN.
Masque de sous-réseau	Entrez le masque de sous-réseau du port WAN.

Passerelle par défaut	Entrez l'adresse IP de la passerelle par défaut.
DNS statique 1	Entrez l'adresse IP du serveur DNS principal.
DNS statique 2	Entrez l'adresse IP du serveur DNS secondaire.

ÉTAPE 4 (Facultatif) Pour configurer les paramètres facultatifs, voir la section **Configurer les paramètres facultatifs**.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Configuration du protocole PPPoE

Configuration du protocole PPPoE

Pour configurer les paramètres PPPoE :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **WAN**.

ÉTAPE 2 Dans le menu déroulant **Type de connexion Internet**, sélectionnez **PPPoE**.

ÉTAPE 3 Saisissez les informations suivantes (contactez le cas échéant votre FAI pour obtenir les informations de connexion PPPoE) :

Nom d'utilisateur	Entrez le nom d'utilisateur fourni par le FAI.
Mot de passe	Entrez le mot de passe fourni par le FAI.
Connexion à la demande	Sélectionnez cette option si votre FAI vous facture en fonction de la durée de connexion. Lorsque vous sélectionnez cette option, la connexion Internet n'est activée qu'en cas de présence de trafic. Si la connexion est en attente (sans trafic en transit), la connexion est désactivée. Si vous cochez **Connexion à la demande**, spécifiez le délai (en minutes) avant déconnexion dans le champ **Durée d'inactivité max**.

Maintenir actif	Lorsque vous cochez cette option, la connexion Internet est toujours active. Dans le champ de délai de renumérotation, spécifiez le délai (en secondes) avant que le Cisco RV110W ne tente de se reconnecter après déconnexion.
Type d'authentification	Sélectionnez le type d'authentification : **Négociation automatique** : le serveur envoie une demande de configuration spécifiant l'algorithme de sécurité paramétré. Le Cisco RV110W renvoie alors ses identifiants d'authentification en utilisant le type de sécurité spécifié par le serveur à l'étape précédente. **PAP** : le Cisco RV110W utilise le protocole PAP (Password Authentication Protocol) lors de la connexion au FAI. **CHAP** : le Cisco RV110W utilise le protocole CHAP (Challenge Handshake Authentication Protocol) lors de la connexion au FAI. **MS-CHAP ou MS-CHAPv2** : le Cisco RV110W utilise le protocole Microsoft Challenge Handshake Authentication Protocol lors de la connexion au FAI.

ÉTAPE 4 (Facultatif) Pour configurer les paramètres facultatifs, voir la section **Configurer les paramètres facultatifs**.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Configuration du protocole PPTP

Configuration du protocole PPTP

Pour configurer les paramètres PPTP :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **WAN**.

ÉTAPE 2 Dans le menu déroulant **Type de connexion Internet**, sélectionnez **PPTP**.

ÉTAPE 3 Saisissez les informations suivantes :

Adresse IP Internet	Entrez l'adresse IP du port WAN.
Masque de sous-réseau	Entrez le masque de sous-réseau du port WAN.
Passerelle par défaut	Entrez l'adresse IP de la passerelle par défaut.
PPTP Server	Saisissez l'adresse IP du serveur PPTP.
Nom d'utilisateur	Entrez le nom d'utilisateur fourni par le FAI.
Mot de passe	Entrez le mot de passe fourni par le FAI.
Connexion à la demande	Sélectionnez cette option si votre FAI vous facture en fonction de la durée de connexion. Lorsque vous sélectionnez cette option, la connexion Internet n'est activée qu'en cas de présence de trafic. Si la connexion est en attente (sans trafic en transit), la connexion est désactivée. Si vous cochez **Connexion à la demande**, spécifiez le délai (en minutes) avant déconnexion dans le champ **Durée d'inactivité max**.
Maintenir actif	Lorsque vous cochez cette option, la connexion Internet est toujours active. Dans le champ de délai de renumérotation, spécifiez le délai (en secondes) avant que le Cisco RV110W ne tente de se reconnecter après déconnexion.

Type d'authentification	Sélectionnez le type d'authentification : **Négociation automatique** : le serveur envoie une demande de configuration spécifiant l'algorithme de sécurité paramétré. Le Cisco RV110W renvoie alors ses identifiants d'authentification en utilisant le type de sécurité spécifié par le serveur à l'étape précédente. **PAP** : le Cisco RV110W utilise le protocole PAP (Password Authentication Protocol) lors de la connexion au FAI. **CHAP** : le Cisco RV110W utilise le protocole CHAP (Challenge Handshake Authentication Protocol) lors de la connexion au FAI. **MS-CHAP ou MS-CHAPv2** : le Cisco RV110W utilise le protocole Microsoft Challenge Handshake Authentication Protocol lors de la connexion au FAI.

ÉTAPE 4 (Facultatif) Pour configurer les paramètres facultatifs, voir la section **Configurer les paramètres facultatifs**.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Configuration du protocole L2TP

Configuration du protocole L2TP

Pour configurer les paramètres L2TP :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **WAN**.

ÉTAPE 2 Dans le menu déroulant **Type de connexion Internet**, sélectionnez **L2TP**.

ÉTAPE 3 Saisissez les informations suivantes :

Adresse IP Internet	Entrez l'adresse IP du port WAN.
Masque de sous-réseau	Entrez le masque de sous-réseau du port WAN.

Passerelle par défaut	Entrez l'adresse IP de la passerelle par défaut.
Serveur L2TP	Entrez l'adresse IP du serveur L2TP.
Nom d'utilisateur	Entrez le nom d'utilisateur fourni par le FAI.
Mot de passe	Entrez le mot de passe fourni par le FAI.
Connexion à la demande	Sélectionnez cette option si votre FAI vous facture en fonction de la durée de connexion. Lorsque vous sélectionnez cette option, la connexion Internet n'est activée qu'en cas de présence de trafic. Si la connexion est en attente (sans trafic en transit), la connexion est désactivée. Si vous cochez **Connexion à la demande**, spécifiez le délai (en minutes) avant déconnexion dans le champ **Durée d'inactivité max**.
Maintenir actif	Lorsque vous cochez cette option, la connexion Internet est toujours active. Dans le champ de délai de renumérotation, spécifiez le délai (en secondes) avant que le Cisco RV110W ne tente de se reconnecter après déconnexion.
Type d'authentification	Sélectionnez le type d'authentification : **Négociation automatique** : le serveur envoie une demande de configuration spécifiant l'algorithme de sécurité paramétré. Le Cisco RV110W renvoie alors ses identifiants d'authentification en utilisant le type de sécurité spécifié par le serveur à l'étape précédente. **PAP** : le Cisco RV110W utilise le protocole PAP (Password Authentication Protocol) lors de la connexion au FAI. **CHAP** : le Cisco RV110W utilise le protocole CHAP (Challenge Handshake Authentication Protocol) lors de la connexion au FAI. **MS-CHAP ou MS-CHAPv2** : le Cisco RV110W utilise le protocole Microsoft Challenge Handshake Authentication Protocol lors de la connexion au FAI.

ÉTAPE 4 (Facultatif) Pour configurer les paramètres facultatifs, voir la section **Configurer les paramètres facultatifs**.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Configurer les paramètres facultatifs

Configurer les paramètres facultatifs

Pour configurer les paramètres facultatifs :

ÉTAPE 1 Dans la section **Paramètres facultatifs**, configurez les paramètres suivants :

Nom d'hôte	Entrez le nom d'hôte du Cisco RV110W.
Domain Name	Entrez le nom de domaine de votre réseau.
MTU	Le MTU (Maximum Transmit Unit) correspond à la taille maximale de paquet pouvant être transmis sur le réseau. La valeur de MTU standard sur les réseaux Ethernet est généralement de 1500 octets. Pour les connexions PPPoE, la valeur est de 1492 octets. À moins que votre FAI impose une modification, Cisco conseille la sélection de l'option **Auto**. Par défaut, la taille de MTU est de 1500 octets. Si votre FAI exige un réglage de MTU personnalisé, sélectionnez **Manuel** et modifiez la taille de MTU.
Taille	Entrez la taille de MTU.

ÉTAPE 2 Cliquez sur **Enregistrer**.

Configuration des paramètres LAN

Les paramètres DHCP et TCP/IP par défaut sont adaptés à la plupart des applications. Si vous souhaitez qu'un autre PC de votre réseau soit le serveur DHCP ou souhaitez configurer les paramètres réseau de tous vos postes, désactivez le DHCP.

Par ailleurs, au lieu d'utiliser un serveur DNS, qui associe les noms de domaines Internet (comme www.cisco.com) à des adresses IP, vous pouvez utiliser un serveur WINS (Windows Internet Naming Service). Un serveur WINS est similaire à un serveur DNS, mais utilise le protocole NetBIOS pour résoudre les noms d'hôte. Le Cisco RV110W inclut l'adresse IP du serveur WINS dans la configuration DHCP envoyée aux clients DHCP.

REMARQUE Si le Cisco RV110W est connecté à un modem ou appareil disposant d'un réseau configuré sur le même sous-réseau (192.168.1.x), le Cisco RV110W modifie automatiquement le sous-réseau du LAN en choisissant une valeur aléatoire basée sur 10.x.x.x, afin d'éviter tout conflit de sous-réseau du côté WAN du Cisco RV110W.

Vous pouvez affecter une adresse IP à chaque sous-réseau logique supplémentaire sur le Cisco RV110W.

Modification de l'adresse IP par défaut du Cisco RV110W

Pour configurer l'adresse IP de LAN par défaut du Cisco RV110W :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **LAN** > **Configuration LAN**.

ÉTAPE 2 Dans la section **IPv4**, saisissez les informations suivantes :

VLAN	Sélectionnez le numéro de VLAN dans le menu déroulant.
Adresse IP locale	Entrez l'adresse IP de LAN du Cisco RV110W. Vérifiez que l'adresse n'est pas utilisée par un autre appareil.
Masque de sous-réseau	Sélectionnez le masque de sous-réseau de la nouvelle adresse IP dans le menu déroulant. La valeur de sous-réseau par défaut est 255.255.255.0.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Lorsque vous modifiez l'adresse IP de LAN du Cisco RV110W, votre PC n'est plus connecté au Cisco RV110W.

ÉTAPE 4 Pour reconnecter votre PC au Cisco RV110W, utilisez l'une des méthodes suivantes :

- Si le Cisco RV110W est configuré en DHCP, libérez et renouvelez l'adresse IP de votre PC.
- Affectez manuellement une adresse IP à votre PC. L'adresse doit appartenir au même sous-réseau que le Cisco RV110W. Par exemple, si vous définissez l'adresse IP du Cisco RV110W sur 10.0.0.1, affectez à votre PC une adresse IP appartenant à la plage 10.0.0.2 à 10.0.0.255.

ÉTAPE 5 Ouvrez une fenêtre de navigateur et entrez la nouvelle adresse IP du Cisco RV110W pour vous reconnecter.

Configuration de DHCP

Par défaut, le Cisco RV110W fonctionne en tant que serveur DHCP pour les hôtes sur le réseau sans fil (ou WLAN) ou filaire (LAN), affecte les adresses IP et fournit les adresses de serveur DNS.

Lorsque le DHCP est activé, l'adresse IP du Cisco RV110W sert d'adresse de passerelle à votre LAN. Le Cisco RV110W affecte des adresses IP aux périphériques réseau sur le LAN à partir d'un groupe d'adresses. Le Cisco RV110W teste chaque adresse avant de l'affecter, afin d'éviter la duplication d'adresses sur le LAN.

Par défaut, le Cisco RV110W affecte une adresse IP à chaque hôte sur le LAN, puisée dans le groupe d'adresses IP par défaut (192.168.1.100 à 192.168.1.149). Si vous devez configurer un hôte avec une adresse IP statique, utilisez une adresse puisée dans le groupe d'adresses IP 192.168.1.2 à 192.168.1.99. Vous évitez ainsi les conflits avec le groupe d'adresses IP par défaut.

Pour configurer les paramètres DHCP :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **LAN** > **Configuration LAN**.

ÉTAPE 2 (Facultatif) Sélectionnez le VLAN que vous souhaitez modifier dans le menu déroulant.

ÉTAPE 3 Dans le champ **Serveur DHCP**, sélectionnez l'une des options suivantes :

Activer	Cliquez sur ce bouton pour autoriser le Cisco RV110W à faire office de serveur DHCP sur le réseau.
Désactiver	Cliquez sur ce bouton pour désactiver DHCP sur le Cisco RV110W. Pour utiliser un autre appareil de votre réseau comme serveur DHCP ou configurer manuellement les paramètres réseau de tous vos postes, désactivez le DHCP.
Relais DHCP	Cliquez sur ce bouton pour sélectionner l'option Relais DHCP afin que le Cisco RV110W relaie les adresses IP d'un autre serveur DHCP.

ÉTAPE 4 Si vous sélectionnez **Activer**, précisez les informations suivantes :

Adresse IP de début	Entrez la première adresse du groupe d'adresses IP. Tout nouveau client DHCP qui rejoint le réseau local reçoit une adresse IP provenant de cette plage (sachant que l'adresse de fin du groupe est fonction de la valeur saisie dans le champ **Nombre maximal d'utilisateurs DHCP**).
Nombre maximal d'utilisateurs DHCP.	Entrez le nombre maximal de clients DHCP.
Plage d'adresses IP	(Lecture seule) Affiche la plage des adresses IP disponibles pour les clients DHCP.
Durée de bail du client	Entrez la durée (en heures) des baux des adresses IP affectés aux clients.
DNS statique 1	Entrez l'adresse IP du serveur DNS principal.
DNS statique 2	Entrez l'adresse IP du serveur DNS secondaire.
DNS statique 3	Entrez l'adresse IP du serveur DNS tertiaire.
WINS	Entrez l'adresse IP du serveur WINS principal.

ÉTAPE 5 Si vous avez sélectionné **Relais DHCP**, entrez l'adresse de la passerelle relais dans le champ **Serveur DHCP distant**. La passerelle relais transmet les messages DHCP entre plusieurs sous-réseaux.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Configuration des VLAN

Un LAN virtuel ou VLAN est un groupe de points d'extrémité d'un réseau, associés par fonction ou selon d'autres caractéristiques communes. Contrairement aux LAN, qui se trouvent généralement sur un même site géographique, les VLAN peuvent regrouper des points d'extrémité indépendamment de l'emplacement physique des appareils et des utilisateurs.

Le Cisco RV110W comporte un VLAN par défaut (VLAN 1), qui ne peut pas être modifié ni changé. Vous pouvez créer quatre autres VLAN sur le Cisco RV110W.

Pour créer un VLAN :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **LAN** > **Membres VLAN**.

ÉTAPE 2 Cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Saisissez les informations suivantes :

ID de VLAN	Entrez l'identifiant numérique du VLAN à affecter aux points d'extrémité des membres du VLAN. La valeur doit être comprise entre 3 et 4094. L'ID de VLAN 1 est réservé au VLAN par défaut, utilisé pour les trames non balisées reçues par l'interface. Les identifiants de VLAN 1 et 2 sont réservés et ne peuvent pas être utilisés.
Description	Entrez une description pour identifier le VLAN.

Port 1 **Port 2** **Port 3** **Port 4**	Vous pouvez associer les VLAN du Cisco RV110W aux ports LAN de l'appareil. Par défaut, les 4 ports appartiennent au VLAN1. Vous pouvez modifier les ports pour les associer à d'autres VLAN. Choisissez le type de trame sortante pour chaque port : **Non balisé** : l'interface est un membre non balisé du VLAN. Les trames du VLAN sont envoyées non balisées au port VLAN. **Balisé** : l'interface est un membre balisé du VLAN. Les trames du VLAN sont envoyées balisées au port VLAN. **Exclu** : le port n'est pas actuellement membre du VLAN. Il s'agit du paramètre par défaut de tous les ports à la création du VLAN.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Pour modifier les paramètres d'un VLAN, sélectionnez le VLAN et cliquez sur **Modifier**. Pour supprimer un VLAN sélectionné, cliquez sur **Supprimer**. Cliquez sur **Enregistrer** pour appliquer les modifications.

Configuration de DHCP statique

Vous pouvez configurer le Cisco RV110W afin qu'il affecte une adresse IP particulière à un appareil doté d'une adresse MAC particulière.

Pour configurer le DHCP statique :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **LAN** > **DHCP statique**.

ÉTAPE 2 Dans le menu déroulant **VLAN**, sélectionnez un numéro de VLAN.

ÉTAPE 3 Cliquez sur **Ajouter une ligne**.

ÉTAPE 4 Saisissez les informations suivantes :

Description	Entrez une description du client.
Adresse IP	Entrez l'adresse IP de l'appareil. L'adresse IP affectée ne doit pas faire partie du groupe d'adresses DHCP configurées. Le groupe DHCP est considéré en tant que groupe générique et toutes les adresses IP réservées doivent être extérieures à ce groupe. L'affectation DHCP statique signifie que le serveur DHCP affecte toujours la même IP à l'adresse MAC d'un appareil lorsque celui-ci se connecte au réseau. Le serveur DHCP sert l'adresse IP réservée lorsque l'appareil doté de l'adresse MAC correspondante demande une adresse IP.
Adresse MAC	Saisissez l'adresse MAC de l'appareil. Le format de l'adresse MAC est XX:XX:XX:XX:XX:XX où X est un chiffre compris entre 0 et 9 (inclus) ou une lettre comprise entre A et F (inclus).

Pour modifier les paramètres d'un client DHCP statique, sélectionnez le client et cliquez sur **Modifier**. Pour supprimer un client DHCP sélectionné, cliquez sur **Supprimer**. Cliquez sur **Enregistrer** pour appliquer les modifications.

Affichage des baux de clients DHCP

Vous pouvez afficher une liste de points d'extrémité sur le réseau (identifiés par nom d'hôte, adresse IP ou adresse MAC) et voir les adresses IP qui leur sont affectées par le serveur DHCP. Le VLAN des points d'extrémité est également affiché.

Pour voir les clients DHCP, sélectionnez **Mise en réseau** > **LAN** > **Baux de clients DHCP**.

Pour chaque VLAN défini sur le Cisco RV110W, une table présente une liste de clients associés au VLAN.

Pour attribuer une adresse IP statique à l'un des périphériques connectés :

ÉTAPE 1 Sur la ligne du périphérique connecté, cochez la case **Ajouter au DHCP statique**.

ÉTAPE 2 Cliquez sur **Enregistrer**.

Le serveur DHCP sur le Cisco RV110W attribue alors toujours l'adresse IP affichée lorsque le périphérique demande une adresse IP.

Configuration d'un hôte de DMZ

Le Cisco RV110W prend en charge les zones démilitarisées ou DMZ. Une DMZ est un sous-réseau ouvert au public, bien que derrière le pare-feu. Une DMZ permet de rediriger des paquets qui arrivent sur l'adresse IP de votre port WAN vers une adresse IP particulière sur votre LAN.

Nous vous conseillons de placer les hôtes devant être exposés au WAN (comme les serveurs Web ou de messagerie) sur le réseau DMZ. Vous pouvez configurer des règles de pare-feu pour autoriser l'accès à des services et ports particuliers sur la DMZ, depuis le LAN et depuis le WAN. En cas d'attaque d'un nœud de la DMZ, le réseau local n'est pas forcément vulnérable.

Vous devez configurer une adresse IP fixe (statique) pour le point d'extrémité qui doit servir d'hôte de la DMZ. Affectez à l'hôte de la DMZ une adresse IP sur le même sous-réseau que l'adresse IP LAN du Cisco RV110W, mais distincte de l'adresse IP donnée à l'interface LAN de cette passerelle.

Pour configurer la DMZ :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **LAN** > **Hôte DMZ**.

ÉTAPE 2 Cochez la case **Activer** pour activer la DMZ sur le réseau.

ÉTAPE 3 Dans le menu déroulant VLAN, sélectionnez l'ID du VLAN sur lequel la DMZ est activée.

ÉTAPE 4 Dans le champ **Adresse IP de l'hôte**, entrez l'adresse IP de l'hôte DMZ. L'hôte DMZ est le point d'extrémité qui reçoit les paquets redirigés.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Configuration de RSTP

Le protocole réseau RSTP (Rapid Spanning Tree Protocol) empêche la formation de boucles dans le réseau et reconfigure de manière dynamique les liaisons physiques qui doivent transférer les trames. Pour configurer le protocole RSTP :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **LAN** > **RSTP**.

ÉTAPE 2 Configurez les paramètres suivants :

Priorité du système	Sélectionnez la priorité système dans le menu déroulant. Vous pouvez choisir une priorité système comprise entre 0 et 61440 en incréments de 4096. Les valeurs autorisées sont 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344 et 61440. Plus la priorité du système est basse, plus le Cisco RV110W a de chance de devenir la racine dans l'arborescence STP. La valeur par défaut est **32768**.
Délai Hello	Le délai Hello correspond à la durée pendant laquelle la racine de l'arborescence STP doit attendre avant d'envoyer des messages de prise de contact. Entrez un nombre entre 1 et 10. La valeur par défaut est **2**.
Délai maximum	Le délai maximum correspond à la durée pendant laquelle le routeur doit attendre avant de recevoir un message de prise de contact. À l'expiration du délai maximum, le routeur essaie de changer l'arborescence STP. Entrez un nombre entre 6 et 40. La valeur par défaut est **20**.

Délai de transfert	Le délai de transfert correspond à l'intervalle au bout duquel une interface passe de l'état de blocage à l'état de réacheminement. Entrez un nombre entre 4 et 30. La valeur par défaut est **15**.
Forcer la version	Sélectionnez la version par défaut du protocole à utiliser. Sélectionnez **Normal** (utiliser RSTP) ou **Compatible** (compatible avec l'ancien STP). La valeur par défaut est **Normal**.

ÉTAPE 3 Dans **Table des paramètres**, configurez les paramètres suivants :

Activer le protocole	Cocher pour activer le RSTP sur le port concerné. RSTP est désactivé par défaut.
Bordure	Cochez pour spécifier que le port concerné est un port de bordure (station terminale). Décochez pour spécifier que le port concerné est un lien (pont) vers un autre appareil STP. L'option Bordure est activée par défaut.
Coût du chemin	Indiquez le coût du chemin RSTP pour les ports concernés. Utilisez 0 pour la valeur par défaut (le Cisco RV110W détermine automatiquement la valeur du chemin). Vous pouvez également entrer une valeur comprise entre 2 et 200 000 000.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Gestion des ports

Vous pouvez configurer les paramètres de vitesse et de contrôle de flux des ports LAN du Cisco RV110W.

Pour configurer la vitesse des ports et le contrôle de flux :

ÉTAPE 1 Sélectionnez **Réseau** > **Gestion des ports**.

ÉTAPE 2 Précisez les informations suivantes :

Port	Le numéro du port.
Lien	La vitesse du port. Lorsqu'aucun appareil n'est branché sur le port, ce champ affiche la mention **Désactivé**.
Mode	Dans le menu déroulant, sélectionnez l'une des vitesses de port suivantes : ▪ **Négociation automatique** : le Cisco RV110W et l'appareil connecté sélectionnent une vitesse commune. ▪ **10 Mbits/s semi** : 10 Mbits/s dans chaque direction, mais dans une seule direction à la fois. ▪ **10 Mbits/s intégral** : 10 Mbits/s dans chaque direction, simultanément. ▪ **100 Mbits/s semi** : 100 Mbits/s dans chaque direction, mais dans une seule direction à la fois. ▪ **100 Mbits/s intégral** : 100 Mbits/s dans chaque direction, simultanément.
Contrôle de flux	Cochez cette case pour activer le contrôle de flux sur le port. Le contrôle de flux consiste à gérer le débit des transmissions de données entre deux nœuds, afin d'empêcher un expéditeur trop rapide de submerger un récepteur trop lent. Il fournit un mécanisme qui permet au récepteur de contrôler la vitesse de transmission, afin que le nœud de réception ne soit pas submergé par les données provenant du nœud de transmission.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Clonage de l'adresse MAC

Parfois, il peut être utile de définir l'adresse MAC du port WAN du Cisco RV110W afin qu'il ait la même adresse MAC que votre PC ou une autre adresse MAC particulière. On appelle cela cloner l'adresse MAC.

Par exemple, certains FAI enregistrent l'adresse MAC de la carte réseau de votre ordinateur lors de l'installation du service. Si vous installez ensuite un routeur derrière le modem câble ou DSL, l'adresse MAC du port WAN du Cisco RV110W n'est pas reconnue par le FAI.

Pour configurer le Cisco RV110W afin qu'il soit reconnu par le FAI, vous devez alors cloner l'adresse MAC du port WAN afin qu'elle corresponde à l'adresse MAC de votre ordinateur.

Pour configurer un clone d'adresse MAC :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **Clone d'adresse MAC**.

ÉTAPE 2 Dans le champ **Clone d'adresse MAC**, cochez la case **Activer**.

ÉTAPE 3 Pour définir l'adresse MAC du port WAN du Cisco RV110W, utilisez l'une des méthodes suivantes :

- Pour régler l'adresse MAC du port WAN sur l'adresse MAC de votre PC, cliquez sur **Cloner MAC du PC**.
- Pour spécifier une autre adresse MAC, entrez-la dans le champ **Adresse MAC**.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration du routage

Configurez les options de routage.

Configuration du mode de fonctionnement

Configuration du mode de fonctionnement

Pour configurer le mode de fonctionnement du Cisco RV110W :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **Routage**.

ÉTAPE 2 Dans le champ **Mode de fonctionnement**, sélectionnez l'une des options suivantes :

Passerelle	(Recommandé) Cliquez sur ce bouton pour que le Cisco RV110W fasse office de passerelle. Conservez ce paramètre par défaut si le Cisco RV110W héberge la connexion Internet de votre réseau et s'il effectue les fonctions de routage.
Routeur	(Pour les utilisateurs expérimentés uniquement) Cliquez sur ce bouton pour que le Cisco RV110W joue le rôle de routeur. Sélectionnez cette option si le Cisco RV110W se trouve sur un réseau doté d'autres routeurs. L'activation du mode Routeur désactive la Traduction d'adresses réseau (ou NAT) sur le Cisco RV110W.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration du routage dynamique

Configuration du routage dynamique

Le protocole RIP (Routing Information Protocol) est un protocole IGP (Interior Gateway Protocol) couramment utilisé sur les réseaux internes. Il permet au routeur d'échanger ses données de routage automatiquement avec d'autres routeurs et d'ajuster dynamiquement ses tables de routages et de s'adapter aux changements sur le réseau.

Le routage dynamique (RIP) permet au Cisco RV110W de s'adapter automatiquement aux modifications physiques de la topologie du réseau et d'échanger des tables de routage avec d'autres routeurs.

Le routeur détermine le chemin suivi par les paquets réseau, en visant le nombre le plus faible possible de sauts entre la source et la destination. RIP est désactivé par défaut.

REMARQUE Le protocole RIP est désactivé par défaut sur le Cisco RV110W.

Pour configurer le routage dynamique :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **Routage**.

ÉTAPE 2 Configurez les paramètres suivants :

RIP	Cochez la case **Activer** pour activer l'option RIP. Le Cisco RV110W peut alors utiliser le protocole RIP pour acheminer le trafic.
Version de paquet RIP envoyé	Sélectionnez la version de paquet RIP envoyé (**RIPv1** ou **RIPv2**). La version de RIP utilisée pour envoyer des mises à jour de routage aux autres routeurs présents sur le réseau dépend de la configuration de ces autres routeurs. RIPv2 est compatible avec RIPv1.
Version de paquet RIP reçu	Sélectionnez la version de paquet RIP reçu.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration du routage statique

Configuration du routage statique

Vous pouvez configurer des routes statiques pour diriger des paquets vers un réseau de destination. Une route statique est un chemin prédéfini devant être emprunté par un paquet afin d'atteindre un hôte ou réseau particulier.

Certains FAI exigent des routes statiques plutôt que des protocoles de routage dynamiques pour la création de tables de routage. Les routes statiques ne requièrent pas de ressources de processeur pour l'échange des informations de routage avec un routeur homologue.

Vous pouvez également utiliser des routes statiques pour atteindre des routeurs homologues qui ne prennent pas en charge les protocoles de routage dynamique. Les routes statiques peuvent être utilisées avec des routes dynamiques. Le Cisco RV110W peut prendre en charge jusqu'à 30 routes statiques.

Prenez garde à ne pas introduire de boucles de routage dans votre réseau.

Pour configurer le routage statique :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **Routage**.

ÉTAPE 2 Dans le menu déroulant **Entrées de route**, sélectionnez une entrée de route.

Pour supprimer une entrée de route, cliquez sur **Supprimer cette entrée**.

ÉTAPE 3 Configurez les paramètres suivants pour l'entrée de route sélectionnée :

Entrer le nom de route	Entrez le nom de la route.
IP du LAN de destination	Entrez l'adresse IP du réseau local de destination.
Masque de sous-réseau	Entrez le masque de sous-réseau du réseau de destination.
Passerelle	Entrez l'adresse IP de la passerelle utilisée pour ce chemin.

Interface	Sélectionnez l'interface vers laquelle les paquets de cette route sont envoyés : ▪ **LAN et sans fil** : cliquez sur ce bouton pour diriger les paquets vers le réseau local et sans fil. ▪ **Internet (WAN)** : cliquez sur ce bouton pour diriger les paquets vers le réseau étendu ou Internet.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configurer le routage inter VLAN

Configurer le routage inter VLAN

Cochez la case du routage inter VLAN pour activer le routage entre les différents VLAN du Cisco RV110W.

Affichage de la table de routage

La table de routage contient des informations sur la topologie du réseau dans l'environnement proche de celui-ci.

Pour afficher les informations de routage sur votre réseau, cliquez sur **Mise en réseau** > **Table de routage** et choisissez l'une des options suivantes :

- **Afficher la table de routage IPv4** : la table de routage est affichée avec les champs configurés sur la page **Mise en réseau** > **Routage**.
- **Afficher la table de routage IPv6** : la table de routage est affichée avec les champs configurés sur les pages **Mise en réseau** > **IPv6**.

Configuration du DNS dynamique

Le DDNS (Dynamic DNS) est un service Internet qui permet de localiser les routeurs dotés d'adresses IP publiques variables à l'aide de noms de domaine Internet. Pour utiliser le DDNS, vous devez créer un compte auprès d'un fournisseur DDNS comme DynDNS.com, TZO.com, 3322.org ou noip.com.

Le routeur notifie des serveurs DNS dynamiques de modifications d'adresses IP WAN, afin que tout service public sur votre réseau puisse être contacté par le biais du nom de domaine.

Pour configurer le DDNS :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **DNS dynamique**.

ÉTAPE 2 Dans le menu déroulant **Service DDNS**, sélectionnez **Désactiver** pour désactiver le service ou sélectionnez le service DDNS à utiliser.

ÉTAPE 3 Si vous n'avez pas de compte DDNS, cliquez sur l'URL du fournisseur DDNS pour visiter son site web et y créer un compte.

ÉTAPE 4 Précisez les informations suivantes :

Adresse e-mail	(TZO.com et noip.com) Entrez l'adresse e-mail utilisée pour créer le compte DDNS.
Nom d'utilisateur	(DynDNS.com et 3322.org) Entrez le nom d'utilisateur du compte DDNS.
Mot de passe	Entrez le mot de passe du compte DDNS.
Vérifier le mot de passe	(TZO.com, DynDNS.com et noip.com) Confirmez le mot de passe du compte DDNS.
Nom d'hôte	(DynDNS.com, 3322.org et noip.com) Entrez le nom d'hôte du serveur DDNS.
Nom de domaine	(TZO.com) Entrez le nom du domaine utilisé pour accéder au réseau.
Adresse IP Internet	(Lecture seule) L'adresse IP Internet du Cisco RV110W.
État	(Lecture seule) L'état n'est affiché qu'en cas de réussite de la mise à jour DDNS ou d'échec de l'envoi des informations de compte au serveur DDNS.

ÉTAPE 5 Pour tester la configuration DDNS, cliquez sur **Tester la configuration**.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Configuration du mode IP

Les propriétés de réseau étendu peuvent être configurées pour les réseaux IPv4 et IPv6. Ces pages vous permettent de saisir des informations sur votre type de connexion Internet et d'autres paramètres.

Pour sélectionner un mode IP :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **Mode IP**.

ÉTAPE 2 Dans le menu déroulant **Mode IP**, sélectionnez l'une des options suivantes :

LAN : IPv4, WAN : IPv4	Faites ce choix pour utiliser l'IPv4 sur les ports LAN et WAN.
LAN : IPv6, WAN : IPv4	Faites ce choix pour utiliser IPv6 sur les ports LAN et IPv4 sur les ports WAN.
LAN : IPv6, WAN : IPv6	Faites ce choix pour utiliser l'IPv6 sur les ports LAN et WAN.
LAN : IPv4+IPv6, WAN : IPv4	Faites ce choix pour utiliser IPv4 et IPv6 sur les ports LAN et IPv4 sur les ports WAN.
LAN : IPv4+IPV6, WAN : IPv4+IPv6	Faites ce choix pour utiliser IPv4 et IPv6 sur les ports LAN et WAN.
LAN : IPv4, WAN : IPv6	Faites ce choix pour utiliser IPv4 sur les ports LAN et IPv6 sur les ports WAN.

ÉTAPE 3 (Facultatif) Si vous utilisez le tunneling 6to4 qui permet la transmission de paquets IPv6 sur un réseau IPv4, procédez comme suit :

a. Cliquez sur **Afficher les champs d'entrée DNS 6to4 statique**.

b. Dans les champs **Domaine** et **IP**, saisissez jusqu'à cinq associations domaine/IP.

La fonction de tunneling 6to4 est généralement utilisé lorsqu'un site ou un utilisateur veut se connecter à l'Internet IPv6 à partir du réseau IPv4 existant.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration d'IPv6

Internet Protocol version 6 (IPv6) est une version du protocole Internet (IP) destinée à remplacer Internet Protocol version 4 (IPv4). La configuration des propriétés WAN d'un réseau IPv6 dépend du type de connexion Internet que vous utilisez.

Configuration du WAN pour un réseau IPv6

Vous pouvez configurer le Cisco RV110W en tant que client DHCPv6 du FAI pour ce WAN ou pour utiliser une adresse IPv6 statique fournie par le FAI.

Configuration du mode IP

Pour configurer les paramètres WAN IPv6 sur votre Cisco RV110W, vous devez d'abord définir le mode IP sur LAN:IPv6, WAN:IPv6 ou LAN:IPv4+IPv6, WAN:IPv4+IPv6.

Pour plus d'informations, reportez-vous à la section **Configuration du mode IP**.

Configuration de DHCPv6

Si votre FAI vous fournit une adresse affectée dynamiquement, configurez le Cisco RV110W en tant que client DHCPv6.

Pour configurer le Cisco RV110W en tant que client DHCPv6 :

ÉTAPE 1 Sélectionnez **Réseau** > **IPv6** > **Configuration WAN IPv6**.

ÉTAPE 2 Dans le champ **Type de connexion WAN**, sélectionnez **Configuration automatique - DHCPv6**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration d'une adresse IP WAN statique

Si votre FAI vous affecte une adresse fixe pour accéder à Internet, configurez le Cisco RV110W afin qu'il utilise une adresse IPv6 statique.

Pour configurer le Cisco RV110W en vue d'utiliser une adresse IPv6 fixe :

ÉTAPE 1 Sélectionnez **Réseau** > **IPv6** > **Configuration WAN IPv6**.

ÉTAPE 2 Dans le champ **Type de connexion WAN**, sélectionnez **IPv6 statique**.

ÉTAPE 3 Saisissez les informations suivantes :

Adresse IPv6	Entrez l'adresse IPv6 du port WAN.
Longueur du préfixe IPv6	Entrez la longueur du préfixe IPv6 définie par le FAI. Le réseau (sous-réseau) IPv6 est identifié par les premiers bits de l'adresse, qui constituent le préfixe. Par exemple, dans l'adresse IP 2001:0DB8:AC10:FE01::, 2001 correspond au préfixe. Tous les hôtes du réseau utilisent les mêmes premiers bits dans leur adresse IPv6. Vous réglez le nombre de bits initiaux communs des adresses du réseau dans ce champ.
Passerelle IPv6 par défaut	Entrez l'adresse IPv6 de la passerelle par défaut. Il s'agit de l'adresse IP du serveur chez le FAI auquel ce routeur se connecte pour accéder à Internet.
DNS statique 1	Entrez l'adresse IP du serveur DNS principal du réseau IPv6 du FAI.
DNS statique 2	Entrez l'adresse IP du serveur DNS secondaire du réseau IPv6 du FAI.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration des paramètres IPv6 PPPoE

Si vous choisissez cette option, les paramètres IPv6 WAN PPPoE doivent correspondre aux paramètres IPv4 WAN PPPoE. Reportez-vous à la section **Configuration du protocole PPPoE**.

Pour configurer les paramètres IPv6 PPPoE du Cisco RV110W :

ÉTAPE 1 Sélectionnez **Réseau** > **IPv6** > **Configuration WAN IPv6**.

ÉTAPE 2 Dans le champ **Type de connexion WAN**, sélectionnez **PPPoE IPv6**.

ÉTAPE 3 Saisissez les informations suivantes (contactez le cas échéant votre FAI pour obtenir les informations de connexion PPPoE) :

Nom d'utilisateur	Entrez le nom d'utilisateur fourni par le FAI.
Mot de passe	Entrez le mot de passe fourni par le FAI.
Connexion à la demande	Sélectionnez cette option si votre FAI vous facture en fonction de la durée de connexion. Lorsque vous sélectionnez cette option, la connexion Internet n'est activée qu'en cas de présence de trafic. Si la connexion est en attente (sans trafic en transit), la connexion est désactivée. Si vous cochez **Connexion à la demande**, spécifiez le délai (en minutes) avant déconnexion dans le champ **Durée d'inactivité max**.
Maintenir actif	Lorsque vous cochez cette option, la connexion Internet est toujours active. Dans le champ de délai de renumérotation, spécifiez le délai (en secondes) avant que le Cisco RV110W tente de se reconnecter après déconnexion.
Type d'authentification	Sélectionnez le type d'authentification : **Négociation automatique** : le serveur envoie une demande de configuration spécifiant l'algorithme de sécurité paramétré. Le Cisco RV110W renvoie alors ses identifiants d'authentification en utilisant le type de sécurité spécifié par le serveur à l'étape précédente. **PAP** : le Cisco RV110W utilise le protocole PAP (Password Authentication Protocol) lors de la connexion au FAI. **CHAP** : le Cisco RV110W utilise le protocole CHAP (Challenge Handshake Authentication Protocol) lors de la connexion au FAI. **MS-CHAP ou MS-CHAPv2** : le Cisco RV110W utilise le protocole Microsoft Challenge Handshake Authentication Protocol lors de la connexion au FAI.

Nom du service	Il est possible que votre FAI dispose d'un nom de service nécessaire pour la connexion au serveur PPPoE. Si c'est le cas, entrez-le ici.
MTU	Le MTU (Maximum Transmit Unit) correspond à la taille maximale de paquet pouvant être transmis sur le réseau. La valeur de MTU standard sur les réseaux Ethernet est généralement de 1500 octets. Pour les connexions PPPoE, la valeur est de 1492 octets. À moins que votre FAI impose une modification, Cisco conseille la sélection de l'option **Auto**. Par défaut, la taille de MTU est de 1500 octets. Si votre FAI exige un réglage de MTU personnalisé, sélectionnez **Manuel** et modifiez la taille de MTU.
Taille	Entrez la taille de MTU.
Mode d'adresse	Choisissez le mode d'adresse dynamique ou statique. Si vous choisissez *dynamique*, entrez l'adresse IPv6 dans le champ ci-dessous.
Longueur du préfixe IPv6	Si vous avez choisi le mode d'adresse *statique*, indiquez la longueur du préfixe IPv6 dans ce champ.
Passerelle IPv6 par défaut	Indiquez l'adresse IP de la passerelle IPv6 par défaut.
DNS statique 1	Si vous avez choisi le mode d'adresse *statique*, indiquez l'adresse IP du serveur DNS principal.
DNS statique 2	Si vous avez choisi le mode d'adresse *statique*, indiquez l'adresse IP du serveur DNS secondaire.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration des paramètres LAN IPv6

En mode IPv6, le serveur DHCP du réseau local (LAN) est activé par défaut (comme en mode IPv4). Le serveur DHCPv6 affecte des adresses IPv6 à partir des groupes d'adresses qui utilisent la longueur de préfixe IPv6 affectée au LAN.

Configuration du mode IP

Pour configurer les paramètres LAN IPv6 sur votre Cisco RV110W, vous devez d'abord régler le mode IP sur l'un des modes suivants :

- LAN : IPv6, WAN : IPv4
- LAN : IPv6, WAN : IPv6
- LAN : IPv4+IPv6, WAN : IPv4
- LAN :IPv4 + IPv6, WAN : IPv4 + IPv6

Pour plus d'informations, reportez-vous à la section **Configuration du mode IP**.

Configuration d'une adresse IP LAN statique

Pour configurer les paramètres de LAN IPv6 :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Configuration LAN IPv6**.

ÉTAPE 2 Saisissez les informations suivantes pour configurer l'adresse IPv6 du LAN :

Adresse IPv6	Entrez l'adresse IPv6 du Cisco RV110W. L'adresse IPv6 par défaut de la passerelle est fec0::1 (ou FEC0:0000:0000:0000:0000:0000:0000:0001). Vous pouvez modifier cette adresse IPv6 de 128 bits en fonction de la configuration de votre réseau.
Longueur du préfixe IPv6	Entrez la longueur de préfixe IPv6. Le réseau (sous-réseau) IPv6 est identifié par les premiers bits de l'adresse, qui constituent le préfixe. Par défaut, le préfixe a une longueur de 64 bits. Tous les hôtes du réseau utilisent les mêmes premiers bits dans leur adresse IPv6. Vous déterminez le nombre de bits initiaux communs des adresses du réseau dans ce champ.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration des paramètres DHCPv6

Pour configurer les paramètres de LAN IPv6 :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Configuration LAN IPv6**.

ÉTAPE 2 Saisissez les informations suivantes pour configurer les paramètres DHCPv6 :

État du DHCP	Cochez cette option pour activer le serveur DHCPv6. Le Cisco RV110W affecte alors une adresse IP appartenant à la plage spécifiée, ainsi que d'autres informations à tout point d'extrémité de LAN qui demande une adresse DHCP.
Nom de domaine	(Facultatif) Entrez le nom de domaine du serveur DHCPv6.
Préférence de serveur	Entrez le niveau de préférences serveur de ce serveur DHCP. Les messages d'annonce DHCP dotés de la valeur de préférence de serveur la plus élevée sont prioritaires sur les autres messages d'annonce DHCP. La valeur par défaut est 255.
DNS statique 1	Entrez l'adresse IPv6 du serveur DNS principal du réseau IPv6 du FAI.
DNS statique 2	Entrez l'adresse IPv6 du serveur DNS secondaire du réseau IPv6 du FAI.
Durée de bail du client	Entrez la durée du bail client. Entrez la durée (en secondes) des baux d'adresses IPv6 destinés aux points d'extrémité du LAN.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration des groupes d'adresses IPv6

Vous pouvez définir le préfixe de délégation IPv6 pour une plage d'adresses IPv6 servies par le serveur DHCPv6 du Cisco RV110W.

En utilisant un préfixe de délégation, vous pouvez automatiser le processus de notification des autres appareils connectés au réseau local d'informations DHCP propres au préfixe affecté.

Pour configurer les groupes d'adresses IPv6 :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Configuration LAN IPv6**.

ÉTAPE 2 Dans la **Table des groupes d'adresses IPv6**, cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Saisissez les informations suivantes :

Adresse de début	Entrez l'adresse IPv6 de début du groupe.
Adresse de fin	Entrez l'adresse IPv6 de fin du groupe.
Longueur du préfixe IPv6	Entrez la longueur de préfixe. Ce champ détermine le nombre de bits initiaux communs des adresses du réseau.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Pour modifier les paramètres d'un groupe, sélectionnez le groupe et cliquez sur **Modifier**. Pour supprimer un groupe sélectionné, cliquez sur **Supprimer**. Cliquez sur **Enregistrer** pour appliquer les modifications.

Configurer le routage IPv6 statique

Vous pouvez configurer des routes statiques pour diriger des paquets vers un réseau de destination. Une route statique est un chemin prédéfini devant être emprunté par un paquet afin d'atteindre un hôte ou réseau particulier.

Certains FAI exigent des routes statiques plutôt que des protocoles de routage dynamiques pour la création de tables de routage. Les routes statiques ne requièrent pas de ressources de processeur pour l'échange des informations de routage avec un routeur homologue.

Vous pouvez également utiliser des routes statiques pour atteindre des routeurs homologues qui ne prennent pas en charge les protocoles de routage dynamique. Les routes statiques peuvent être utilisées avec des routes dynamiques. Prenez garde à ne pas introduire de boucles de routage dans votre réseau.

Pour créer une route statique :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **IPv6 Routage statique**.

ÉTAPE 2 Dans la liste des routes statiques, cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Saisissez les informations suivantes :

Nom	Saisissez le nom de la route.
Destination	Entrez l'adresse IPv6 de l'hôte ou réseau de destination pour ce chemin.
Longueur du préfixe	Entrez le nombre de bits de préfixe de l'adresse IPv6 qui définissent le sous-réseau de destination.
Passerelle	Entrez l'adresse IPv6 de la passerelle par laquelle l'hôte ou réseau de destination est joignable.
Interface	Sélectionnez l'interface pour la route dans le menu déroulant : **LAN**, **WAN** ou **6to4**.
Métrique	Entrez la priorité du chemin en choisissant une valeur entre 2 et 15. S'il existe plusieurs routes vers une même destination, la route avec la métrique la plus fiable est utilisée.
Actif	Cochez cette option pour activer la route. Lorsque vous ajoutez une route dans un état inactif, elle est ajoutée à la table de routage, mais elle n'est pas utilisée par le Cisco RV110W. Vous pouvez alors activer la route ultérieurement. Cette option est pratique si le réseau auquel accède la route n'est pas disponible lorsque vous l'ajoutez. Une fois le réseau disponible, vous pouvez activer la route.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Pour modifier les paramètres d'une route, sélectionnez-la et cliquez sur **Modifier**. Pour supprimer une route sélectionnée, cliquez sur **Supprimer**. Cliquez sur **Enregistrer** pour appliquer les modifications.

Configuration du routage (RIPng)

RIP Next Generation (RIPng) est un protocole de routage basé sur l'algorithme D-V (Distance Vector). RIPng utilise des paquets UDP pour échanger des informations de routage par le port 521.

Le protocole RIPng utilise un nombre de sauts pour mesurer la distance jusqu'à la destination. Le nombre de sauts est appelé mesure, métrique ou coût. Le nombre de sauts d'un routeur vers un réseau auquel il est directement connecté est 0. Le nombre de sauts entre deux routeurs directement connectés est 1. Lorsque le nombre de sauts est supérieur ou égal à 16, le réseau ou hôte de destination est injoignable.

Par défaut, l'actualisation du routage est envoyée toutes les 30 secondes. Si le routeur ne reçoit pas de mise à jour de routage d'un voisin après 180 secondes, les routes obtenues du voisin sont considérées comme injoignables. Si aucune mise à jour de routage n'est reçue après 240 secondes de plus, le routeur supprime ces chemins de la table de routage.

Sur le Cisco RV110W, Le protocole RIPng est désactivé par défaut.

Pour configurer le protocole RIPng :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Routage (RIPng)**.

ÉTAPE 2 Cochez **Activer**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration du tunneling

Tunneling 6to4

Le tunneling IPv6 vers IPv4 (tunneling 6-to-4) permet la transmission de paquets IPv6 sur un réseau IPv4. Le tunneling 6-to-4 est généralement utilisé lorsqu'un site ou un utilisateur veut se connecter à l'Internet IPv6 à partir du réseau IPv4 existant.

Pour configurer le tunneling 6-to-4 :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Tunneling**.

ÉTAPE 2 Dans le champ **Tunneling 6 to 4**, cochez la case **Activer**.

ÉTAPE 3 Choisissez le type de tunneling (**6to4** ou **6RD** [Rapid Deployment]).

ÉTAPE 4 Pour le tunneling 6RD, choisissez **automatique** ou **manuelle**.

ÉTAPE 5 Saisissez les informations suivantes :

- **Préfixe IPv6**
- **Longueur du préfixe IPv6**
- **Border Relay**
- **Longueur du masque IPv4**

ÉTAPE 6 Cliquez sur **Enregistrer**.

Tunneling 6to4

Le tunneling IPv4 vers IPv6 (tunneling 4-to-6) permet la transmission de paquets IPv4 sur un réseau IPv6. Pour configurer le tunneling 4-to-6 :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Tunneling**.

ÉTAPE 2 Dans le champ **Tunneling 4 to 6**, cochez la case **Activer**.

ÉTAPE 3 Entrez l'adresse IPv6 du WAN local sur le Cisco RV110W.

ÉTAPE 4 Entrez l'adresse IPv6 distante ou l'adresse IP du point d'extrémité distant.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Affichage de l'état du tunnel IPv6

Pour afficher l'état du tunnel IPv6 :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **État du tunnel IPv6**.

ÉTAPE 2 Cliquez sur **Actualiser** pour afficher les dernières informations.

Cette page affiche des informations sur le tunnel automatique établi sur l'interface WAN dédiée. La table indique le nom du tunnel et l'adresse IPv6 créée sur l'appareil.

Configuration de l'annonce du routeur

Le démon RADVD (Router Advertisement Daemon) sur le Cisco RV110W est à l'écoute des messages de sollicitation du routeur sur le LAN IPv6 et répond par des annonces de routeur selon les besoins. Il s'agit d'une configuration IPv6 automatique sans état et le Cisco RV110W distribue les préfixes IPv6 à tous les nœuds du réseau.

Pour configurer le RADVD :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Annonce de routeur**.

ÉTAPE 2 Saisissez les informations suivantes :

État RADVD	Sélectionnez **Activer** pour activer le RADVD.
Mode d'annonce	Sélectionnez l'un des modes suivants : **Multidiffusion non sollicitée** : sélectionnez ce mode pour envoyer les annonces du routeur (RA) à toutes les interfaces appartenant au groupe de multidiffusion. **Destination unique seulement** : sélectionnez ce mode pour limiter les annonces à des adresses IPv6 bien connues (les annonces du routeur ne sont envoyées qu'à l'interface appartenant à l'adresse connue).

Intervalle d'annonce	Si vous sélectionnez le mode d'annonce **Multidiffusion non demandée**, entrez l'intervalle d'annonce (4 à 1800). La valeur par défaut est **30**. L'intervalle d'annonce est une valeur aléatoire comprise entre les valeurs minimales et maximales d'intervalle d'annonce (MinRtrAdvInterval et MaxRtrAdvInterval). MinRtrAdvInterval = 0,33 * MaxRtrAdvInterval
Indicateurs d'annonces	Cochez la case **Gérés** pour utiliser le protocole administré / avec état pour la configuration automatique des adresses. Cochez la case **Autre** pour utiliser le protocole administré / avec état pour la configuration automatique d'autres informations (autre que l'adresse).
Préférence de routeur	Sélectionnez **faible**, **moyen** ou **élevé** dans le menu déroulant. La valeur par défaut est **moyen**. La préférence de routeur fournit une mesure de préférence pour les routeurs par défaut. Les valeurs basse, moyenne et élevée sont signalées à l'aide de bits non utilisés dans les messages d'annonce du routeur. Cette extension est rétrocompatible, tant avec les routeurs (réglage de la valeur de préférence de routeur) qu'avec les hôtes (interprétation de la valeur de préférence de routeur). Ces valeurs sont ignorées par les hôtes qui ne mettent pas en œuvre la préférence de routeur. Cette fonctionnalité est pratique lorsque d'autres appareils utilisant le RADVD sont présents sur le réseau local.

MTU	Entrez la taille de MTU (0 ou 1280 à 1500). La valeur par défaut est **1500** octets. Le MTU correspond au paquet le plus volumineux pouvant être transmis sur le réseau. Le MTU est utilisé dans les annonces du routeur pour assurer que tous les nœuds du réseau utilisent la même valeur de MTU lorsque le MTU du réseau n'est pas connu.
Durée de vie du routeur	Entrez la valeur de durée de vie du routeur ou la durée en secondes d'existence des messages d'annonce sur le chemin. La valeur par défaut est **3600** secondes.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration des préfixes d'annonce

Pour configurer les préfixes RADVD disponibles :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Préfixes d'annonce**.

ÉTAPE 2 Cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Saisissez les informations suivantes :

Type de préfixe IPv6	Sélectionnez l'un des types suivants dans le menu déroulant : **6to4** : 6to4 est un système qui permet la transmission de paquets IPv6 sur un réseau IPv4. Il est utilisé lorsqu'un utilisateur veut se connecter à l'Internet IPv6 en passant par son réseau IPv4 existant. **Global/local** : une adresse IPv6 locale unique que vous pouvez utiliser sur les réseaux IPv6 privés ou une adresse Internet IPv6 unique globale.

ID SLA	Si vous sélectionnez le type de préfixe IPv6 **6to4**, entrez l'ID SLA (identifiant Site-Level Aggregation). L'ID SLA du préfixe d'adresse 6to4 est réglé sur l'ID de l'interface sur laquelle les annonces sont envoyées.
Préfixe IPv6	Si vous sélectionnez le type de préfixe IPv6 **Global/local**, entrez le préfixe IPv6. Le préfixe IPv6 spécifie l'adresse réseau IPv6.
Longueur du préfixe IPv6	Si vous sélectionnez le type de préfixe IPv6 **Global/local**, entrez la longueur de préfixe. La variable de longueur de préfixe est une valeur décimale qui indique le nombre de bits contigus les plus significatifs de l'adresse qui composent la partie réseau de l'adresse.
Durée de vie du préfixe	Entrez la durée de vie du préfixe ou la durée durant laquelle le routeur à l'origine de la demande est autorisé à utiliser le préfixe.

ÉTAPE 4 Cliquez sur **Enregistrer**.

3

Configuration du réseau sans fil

Ce chapitre indique la marche à suivre pour configurer les paramètres de réseau sans fil du Cisco RV110W.

- **Sécurité sans fil**
- **Réseaux sans fil Cisco RV110W**
- **Configuration des paramètres sans fil de base**
- **Configuration des paramètres sans fil avancés**
- **Configuration de WDS**
- **Configuration de WPS**

Sécurité sans fil

Les réseaux sans fil sont pratiques et faciles à créer, ce qui explique que les particuliers et les professionnels équipés d'un accès haut débit à Internet y ont de plus en plus recours.

Les réseaux sans fil fonctionnent cependant en transmettant les informations par ondes radio, ce qui les rend potentiellement plus vulnérables que les réseaux traditionnels filaires.

Conseils relatifs à la sécurité des réseaux sans fil

Conseils relatifs à la sécurité des réseaux sans fil

Vous ne pouvez pas empêcher quelqu'un de se connecter à votre réseau sans fil, mais vous pouvez suivre les conseils suivants pour sécuriser votre réseau :

- Modifiez le nom ou SSID par défaut du réseau sans fil.

Les appareils sans fil sont dotés d'un nom ou SSID de réseau sans fil par défaut. Il s'agit du nom de votre réseau sans fil, qui peut comporter jusqu'à 32 caractères.

Pour protéger votre réseau, modifiez le nom de réseau sans fil par défaut et donnez-lui un nom unique qui le distingue des autres réseaux sans fil qui vous entourent.

Lorsque vous choisissez un nom, n'utilisez pas d'informations personnelles (comme un numéro de carte bancaire), car cette information sera visible par tout individu qui parcourt les réseaux sans fil.

- Modifiez le mot de passe par défaut.

  Sur les appareils sans fil comme les points d'accès, routeurs et passerelles, vous devez saisir un mot de passe lorsque vous souhaitez modifier les paramètres. Ces appareils ont un mot de passe par défaut. Le mot de passe par défaut est souvent **cisco**.

  Les pirates connaissent ces valeurs par défaut et essaient de les exploiter pour accéder à vos appareils sans fil et modifier vos paramètres réseau. Pour empêcher les accès non autorisés, personnalisez le mot de passe de l'appareil afin qu'il soit difficile à deviner.

- Activez le filtrage des adresses MAC.

  Les routeurs et passerelles Cisco vous permettent d'activer le filtrage d'adresses MAC. L'adresse MAC est une série unique de chiffres et de lettres affectée à chaque appareil en réseau.

  Lorsque le filtrage des adresses MAC est activé, l'accès au réseau sans fil est réservé aux appareils sans fil dotés d'adresses MAC particulières. Vous pouvez par exemple spécifier l'adresse MAC de chaque ordinateur de votre réseau, afin que seuls ces ordinateurs puissent accéder à votre réseau sans fil.

- Activez le chiffrement.

  Le chiffrement protège les données transmises sur un réseau sans fil. Les normes WPA/WPA2 (Wi-Fi Protected Access) et WEP (Wired Equivalency Privacy) offrent différents niveaux de sécurité pour la communication sans fil. Actuellement, les appareils certifiés Wi-Fi sont tenus de prendre en charge le WPA2, mais ne sont pas obligés de prendre en charge le WEP.

  Un réseau chiffré par WPA/WPA2 est mieux sécurisé qu'un réseau chiffré en WEP, car le WPA/WPA2 utilise le chiffrement par clé dynamique.

Pour protéger les données qui transitent par les ondes, activez le niveau de chiffrement le plus élevé pris en charge par vos équipements réseau.

WEP est une norme de chiffrement plus ancienne, mais certains appareils plus anciens n'offrent que cette option et ne prennent pas en charge le WPA.

- Ne placez pas les routeurs, points d'accès et passerelles sans fil près des murs extérieurs et des fenêtres.
- Éteignez les routeurs, points d'accès et passerelles sans fil lorsque vous ne les utilisez pas (la nuit, pendant les vacances).
- Utilisez des mots de passe complexes contenant au moins huit caractères. Combinez chiffres et lettres pour éviter l'utilisation de mots existants dans le dictionnaire.

Directives générales sur la sécurité réseau

Directives générales sur la sécurité réseau

Inutile de sécuriser le réseau sans fil si le réseau sous-jacent n'est pas sécurisé. Cisco vous recommande de prendre les précautions suivantes :

- Protégez tous les ordinateurs sur le réseau et protégez individuellement les fichiers confidentiels par mot de passe.
- Modifiez les mots de passe à intervalles réguliers.
- Installez des logiciels antivirus et des logiciels de pare-feu individuels.
- Désactivez le partage de fichiers en point à point pour empêcher son utilisation par des applications sans votre accord.

Réseaux sans fil Cisco RV110W

Le Cisco RV110W fournit quatre réseaux sans fil virtuels ou quatre SSID (Service Set Identifier) : ciscosb1, ciscosb2, ciscosb3 et ciscosb4. Il s'agit des noms ou SSID par défaut de ces réseaux, mais vous pouvez les renommer à votre guise. Le tableau suivant décrit les paramètres par défaut de ces réseaux :

Nom SSID	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Activé	Oui	Non	Non	Non
Diffusion SSID	Activé	Désactivé	Désactivé	Désactivé
Mode de sécurité	Désactivé[1]	Désactivé	Désactivé	Désactivé
Filtre MAC	Désactivé	Désactivé	Désactivé	Désactivé
VLAN	1	1	1	1
Isolation sans fil avec SSID	Désactivé	Désactivé	Désactivé	Désactivé
WMM	Activé	Activé	Activé	Activé
Bouton matériel WPS	Activé	Désactivé	Désactivé	Désactivé

1. Lorsque vous utilisez l'assistant de configuration, sélectionnez **Sécurité optimale** ou **Meilleure sécurité** pour protéger le Cisco RV110W contre les accès non autorisés.

Configuration des paramètres sans fil de base

Utilisez la page **Paramètres de base** (**Sans fil** > **Paramètres de base**) pour configurer les principaux paramètres sans fil.

Pour configurer les paramètres sans fil de base :

ÉTAPE 1 Sélectionnez **Sans fil** > **Paramètres de base**.

ÉTAPE 2 Dans le champ **Radio**, cochez la case **Activer** pour activer la radio sans fil. Par défaut, un seul réseau sans fil est activé, **ciscosb1**.

ÉTAPE 3 Dans le champ **Mode de réseau sans fil**, sélectionnez l'une des options suivantes dans le menu déroulant :

Mixte B/G/N	Sélectionnez cette option si vous avez des appareils sans fil de type N, B et G sur votre réseau. Il s'agit de la valeur par défaut (recommandée).
B seulement	Sélectionnez cette option si vous n'avez que des appareils sans fil de type B sur votre réseau.
G seulement	Sélectionnez cette option si vous n'avez que des appareils sans fil de type G sur votre réseau.
N seulement	Sélectionnez cette option si vous n'avez que des appareils sans fil de type N sur votre réseau.
Mixte B/G	Sélectionnez cette option si vous n'avez que des appareils sans fil de type B et G sur votre réseau.
G/N mixte	Sélectionnez cette option si vous n'avez que des appareils sans fil de type G et N sur votre réseau.

ÉTAPE 4 Si vous choisissez **Mixte B/G/N**, **N seulement** ou **Mixte G/N**, dans le champ **Sélection de bande sans fil**, sélectionnez la bande sans fil de votre réseau (**20 MHz** ou **20/40 MHz**). Si vous avez choisi N seulement, vous devez utiliser la sécurité WPA2 sur votre réseau. Reportez-vous à la section **Configurer le mode de sécurité**.

ÉTAPE 5 Dans le champ **Canal sans fil**, sélectionnez le canal sans fil dans le menu déroulant.

ÉTAPE 6 Dans le champ **VLAN de gestion PA**, sélectionnez VLAN 1 si vous utilisez les paramètres par défaut.

Pour créer des VLAN supplémentaires, sélectionnez une valeur correspondant aux VLAN configurés sur d'autres commutateurs du réseau. Il s'agit d'une mesure de sécurité. Il peut également être nécessaire de changer le VLAN de gestion pour limiter l'accès au gestionnaire de dispositifs du Cisco RV110W.

ÉTAPE 7 (Facultatif) Dans le champ **U-APSD (économies d'énergie WMM)**, cochez la case **Activer** pour activer la fonction U-APSD (Unscheduled Automatic Power Save Delivery), également appelée WMM Power Save (économies d'énergie WMM), qui limite l'énergie consommée par les ondes radio.

U-APSD est un mécanisme d'économie d'énergie conçue pour les applications en temps réel, comme la VoIP, qui transfèrent les données en duplex intégral sur Internet. En classifiant le trafic IP sortant en tant que données *Voix*, les applications de ce type peuvent améliorer l'autonomie d'environ 25 % tout en limitant les délais de transmission.

ÉTAPE 8 (Facultatif) Configurez les paramètres des quatre réseaux sans fil (voir la section **Modification des paramètres de réseau sans fil**).

ÉTAPE 9 Cliquez sur **Enregistrer**.

Modification des paramètres de réseau sans fil

La **Table sans fil** de la page **Paramètres de base** (**Sans fil** > **Paramètres de base**) présente les paramètres des quatre réseaux sans fil pris en charge par le Cisco RV110W.

Pour configurer ces paramètres de réseau sans fil :

ÉTAPE 1 Cochez les cases des réseaux que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur le bouton **Modifier**.

ÉTAPE 3 Configurez les paramètres suivants :

Activer SSID	Cliquez sur **Activé** pour activer le réseau.
Nom SSID	Nommez le réseau.
Diffusion SSID	Cochez cette case pour activer la diffusion du SSID. Si la diffusion du SSID est activée, le routeur sans fil annonce sa disponibilité aux périphériques sans fil dans la plage du routeur.
VLAN	Sélectionnez le VLAN associé au réseau.
Isolation sans fil avec SSID	Cochez cette case pour activer l'isolation sans fil au sein du SSID.
WMM (Wi-Fi Multimedia)	Cochez cette case pour activer le WMM.
Bouton matériel WPS	Cochez cette case pour associer le bouton WPS de la façade du Cisco RV110W à ce réseau.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configurer le mode de sécurité

Vous pouvez configurer l'un des modes de sécurité suivant pour les réseaux sans fil :

Configuration de WEP

Le mode de sécurité WEP offre une sécurité faible en utilisant une méthode de chiffrement simple et moins sûre que le WPA. La méthode WEP peut être nécessaire si vos appareils ne prennent pas en charge le WPA.

REMARQUE Si vous n'êtes pas obligé d'utiliser le WEP, nous vous conseillons d'utiliser le WPA2. Si vous utilisez le mode sans fil N seulement, vous devez activer WPA2.

Pour configurer le mode de sécurité WEP :

ÉTAPE 1 Dans la **Table sans fil** (**Sans fil** > **Paramètres de base**), cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Modifier le mode de sécurité**.

La page **Paramètres de sécurité** apparaît.

ÉTAPE 3 Dans le champ **Sélectionner un SSID**, sélectionnez le SSID dont vous souhaitez configurer les paramètres de sécurité.

ÉTAPE 4 Dans le menu **Mode de sécurité**, sélectionnez **WEP**.

ÉTAPE 5 Dans le champ **Type d'authentification**, sélectionnez l'une des options suivantes :

- **Système ouvert** : il s'agit de l'option par défaut.
- **Clé partagée** : sélectionnez cette option si votre administrateur réseau vous le demande. Dans le doute, sélectionnez l'option par défaut.

Dans les deux cas, les clients sans fil doivent fournir la bonne clé partagée (mot de passe) pour accéder au réseau sans fil.

ÉTAPE 6 Dans le champ **Chiffrement**, sélectionnez le type de chiffrement :

- **10/64 bits (10 chiffres hexadécimaux) :** fournit une clé sur 40 bits.
- **26/128 bits (26 chiffres hexadécimaux)** : fournit une clé sur 104 bits, soit un code plus difficile à déchiffrer. Nous recommandons le chiffrement sur 128 bits.

ÉTAPE 7 (Facultatif) Dans le champ **Mot de passe**, entrez une expression alphanumérique (de plus de huit caractères pour une sécurité optimale) et cliquez sur **Générer** pour créer quatre clés WEP uniques dans les champs Clé WEP.

Si vous préférez fournir votre propre clé, entrez-la directement dans le champ **Clé 1** (recommandé). La clé doit avoir une longueur de 5 caractères ASCII (ou 10 caractères hexadécimaux) pour le WEP 64 bits ou de 13 caractères ASCII (ou 26 caractères hexadécimaux) pour le WEP 128 bits. Les caractères hexadécimaux valables sont compris entre 0 et 9 et A et F.

ÉTAPE 8 Dans le champ **Clé transmise**, sélectionnez la clé que les appareils devront utiliser comme clé partagée pour accéder au réseau sans fil.

ÉTAPE 9 Cliquez sur **Enregistrer** pour enregistrer vos paramètres.

ÉTAPE 10 Cliquez sur **Retour** pour revenir à la page **Paramètres de base**.

Configuration de WPA-Personal, WPA2-Personal et de WPA2-Personal mixte

Les modes de sécurité WPA Personnel, WPA2 Personnel et WPA2 Personnel mixte fournissent une sécurité forte pour remplacer le WEP.

- **WPA-Personnel** : WPA fait partie de la norme de sécurité sans fil (802.11i) homologuée par la Wi-Fi Alliance. Elle a été conçue en tant que standard intermédiaire pour remplacer le WEP pendant l'élaboration de la norme 802.11i. WPA-Personnel est compatible avec le chiffrement TKIP (Temporal Key Integrity Protocol) et AES (Advanced Encryption Standard).
- **WPA2-Personnel** : (Recommandé) WPA2 est la norme de sécurité spécifiée par la norme 802.11i finalisée. WPA2 prend en charge le chiffrement AES et utilise une clé prépartagée (PSK) pour l'authentification.
- **WPA2-Personnel mixte** : permet aux clients WPA et WPA2 de se connecter simultanément en utilisant l'authentification PSK.

L'authentification personnelle correspond à la clé prépartagée qui est un mot de passe alphanumérique partagé avec le poste sans fil.

Pour configurer le mode de sécurité WPA Personnel :

ÉTAPE 1 Dans la **Table sans fil** (**Sans fil** > **Paramètres de base**), cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Modifier le mode de sécurité**. La page **Paramètres de sécurité** apparaît.

ÉTAPE 3 Dans le champ **Sélectionner un SSID**, sélectionnez le SSID dont vous souhaitez configurer les paramètres de sécurité.

ÉTAPE 4 Dans le menu **Mode de sécurité**, sélectionnez l'une des trois options WPA Personnel.

ÉTAPE 5 (WPA-Personnel seulement) Dans le champ **Chiffrement**, sélectionnez l'une des options suivantes :

- **TKIP/AES** : sélectionnez **TKIP/AES** pour assurer la compatibilité avec des appareils sans fil plus anciens qui ne prennent pas nécessairement en charge AES.
- **AES** : cette option offre une meilleure sécurité.

ÉTAPE 6 Dans le champ **Clé de sécurité**, entrez une expression alphanumérique (8 à 63 caractères ASCII ou 64 chiffres hexadécimaux). L'échelle d'évaluation de la sécurité du mot de passe indique la robustesse de la clé : Inférieur au seuil minimum, Faible, Fort, Très fort ou Sécurisé. Nous vous recommandons d'utiliser une clé de sécurité considérée comme sécurisée sur l'échelle d'évaluation.

ÉTAPE 7 Pour afficher la clé de sécurité à mesure que vous la saisissez, cochez la case **Afficher le mot de passe**.

ÉTAPE 8 Dans le champ **Renouvellement de clé**, entrez l'intervalle de renouvellement de la clé (de 600 à 7 200 secondes). La valeur par défaut est 3600.

ÉTAPE 9 Cliquez sur **Enregistrer** pour enregistrer vos paramètres.

ÉTAPE 10 Cliquez sur **Retour** pour revenir à la page **Paramètres de base**.

Configuration des modes WPA-Enterprise, WPA2-Enterprise et WPA2-Enterprise mixte

Les modes de sécurité WPA Entreprise, WPA2 Entreprise et WPA2 Entreprise mixte permettent d'utiliser l'authentification serveur RADIUS.

- **WPA-Entreprise** : permet d'utiliser le WPA avec authentification serveur RADIUS.
- **WPA2-Entreprise** : permet d'utiliser le WPA2 avec authentification serveur RADIUS.
- **WPA2-Entreprise mixte** : permet aux clients WPA et WPA2 de se connecter simultanément en utilisant l'authentification RADIUS.

Pour configurer le mode de sécurité WPA Entreprise :

ÉTAPE 1 Dans la **Table sans fil** (**Sans fil** > **Paramètres de base**), cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Modifier le mode de sécurité**.

ÉTAPE 3 Dans le champ **Sélectionner un SSID**, sélectionnez le SSID dont vous souhaitez configurer les paramètres de sécurité.

ÉTAPE 4 Dans le menu **Mode de sécurité**, sélectionnez l'une des trois options WPA Entreprise.

ÉTAPE 5 (WPA-Entreprise seulement) Dans le champ **Chiffrement**, sélectionnez l'une des options suivantes :

- **TKIP/AES** : sélectionnez **TKIP/AES** pour assurer la compatibilité avec des appareils sans fil plus anciens qui ne prennent pas nécessairement en charge AES.
- **AES** : cette option offre une meilleure sécurité.

ÉTAPE 6 Dans le champ **Serveur RADIUS**, entrez l'adresse IP du serveur RADIUS.

ÉTAPE 7 Dans le champ **Port RADIUS**, entrez le port utilisé pour accéder au serveur RADIUS.

ÉTAPE 8 Dans le champ **Clé partagée**, entrez une expression alphanumérique (8 à 63 caractères ASCII ou 64 chiffres hexadécimaux).

ÉTAPE 9 Dans le champ **Renouvellement de clé**, entrez l'intervalle de renouvellement de la clé (de 600 à 7 200 secondes). La valeur par défaut est 3600.

ÉTAPE 10 Cliquez sur **Enregistrer** pour enregistrer vos paramètres.

ÉTAPE 11 Cliquez sur **Retour** pour revenir à la page **Paramètres de base**.

Configuration du filtrage MAC

Vous pouvez utiliser le filtrage MAC pour accorder ou refuser l'accès au réseau sans fil en fonction de l'adresse MAC (matérielle) de l'appareil qui demande l'accès. Vous pouvez par exemple entrer les adresses MAC d'un ensemble d'ordinateurs et n'autoriser l'accès au réseau qu'à ces ordinateurs. Vous pouvez configurer le filtrage MAC pour chaque réseau ou SSID.

Pour configurer le filtrage MAC :

ÉTAPE 1 Dans la **Table sans fil** (**Sans fil** > **Paramètres de base**), cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Modifier le filtrage MAC**. La page **Filtre MAC sans fil** apparaît.

ÉTAPE 3 Dans le champ **Modifier le filtrage MAC**, cochez la case **Activer** pour activer le filtrage MAC pour le SSID actuel.

ÉTAPE 4 Dans le champ **Contrôle de connexion**, sélectionnez le type d'accès au réseau sans fil :

- **Interdire** : sélectionnez cette option pour empêcher les appareils dont les adresses MAC sont incluses dans la **Table d'adresses MAC** d'accéder au réseau sans fil. Cette option est sélectionnée par défaut.
- **Autoriser** : sélectionnez cette option pour autoriser les appareils dont les adresses MAC sont incluses dans la **Table d'adresses MAC** à accéder au réseau sans fil.

ÉTAPE 5 Pour afficher les ordinateurs et autres appareils sur le réseau sans fil, cliquez sur **Afficher la liste des clients**.

ÉTAPE 6 Dans le champ **Enregistrer dans la liste de filtrage des adresses MAC**, cochez la case pour ajouter l'appareil à la liste des appareils à ajouter à la **Table d'adresses MAC**.

ÉTAPE 7 Cliquez sur **Ajouter à l'adresse MAC** pour ajouter les appareils sélectionnés à la **Liste des clients** de la **Table d'adresses MAC**.

ÉTAPE 8 Cliquez sur **Enregistrer** pour enregistrer vos paramètres.

ÉTAPE 9 Cliquez sur **Retour** pour revenir à la page **Paramètres de base**.

Configuration de l'accès par horaire

Pour renforcer la protection de votre réseau, vous pouvez restreindre l'accès en spécifiant les heures auxquelles les utilisateurs peuvent accéder au réseau.

Pour configurer l'accès par horaire :

ÉTAPE 1 Dans la **Table sans fil** (**Sans fil** > **Paramètres de base**), cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Accès par horaire**. La page Accès par horaire apparaît.

ÉTAPE 3 Dans le champ **Durée d'activité**, cochez la case **Activer** pour activer l'accès par horaire.

ÉTAPE 4 Dans les champs **Heure de début** et **Heure de fin**, spécifiez la plage horaire durant laquelle l'accès au réseau sera autorisé.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Configuration du réseau invité sans fil

Le Cisco RV110W prend en charge un réseau « invité » sans fil qui est distinct des autres SSID, ou réseaux, sans fil sur le routeur. Ce routeur assure un accès invité sécurisé qui est isolé du reste du réseau et qui peut être configuré pour restreindre le temps d'accès et la bande passante utilisée. Les restrictions et les recommandations de configuration suivantes s'appliquent :

- Un réseau invité peut être configuré pour chaque Cisco RV110W.
- Le réseau invité est configuré en tant que l'un des quatre SSID disponibles sur le Cisco RV110W.
- Il n'est pas possible de configurer le réseau invité sur le VLAN de gestion PA (VLAN ID 1).

Pour configurer le réseau invité :

Pour créer un nouveau VLAN :

ÉTAPE 1 Dans l'interface de gestion, sélectionnez **Mise en réseau** > **LAN** > **Appartenance VLAN**.

ÉTAPE 2 Dans la *table des paramètres de réseau VLAN*, ajoutez un nouveau VLAN pour le réseau invité. Par exemple, cliquez sur **Ajouter une ligne** et entrez ce qui suit :

- **ID VLAN** : entrez un numéro pour le VLAN (par exemple, **4**).
- **Description** : entrez le nom du VLAN (par exemple, **réseau-invité**).

ÉTAPE 3 Conservez les **balises** des ports et cliquez sur **Enregistrer**.

Pour configurer le réseau invité :

ÉTAPE 1 Dans l'interface de gestion, choisissez **Sans fil** > **Paramètres de base**.

ÉTAPE 2 Dans la *Table sans fil*, sélectionnez le SSID ou le réseau que vous souhaitez désigner comme réseau invité.

ÉTAPE 3 Cliquez sur **Modifier**. Modifiez le nom du SSID pour qu'il reflète la désignation « invité » (par exemple, « *réseau-invité* »).

ÉTAPE 4 Cochez la case *Diffusion SSID* pour que le réseau apparaisse en tant que connexion sans fil pour les clients recherchant des réseaux.

ÉTAPE 5 Cochez la case *Réseau invité* pour configurer ce SSID en tant que réseau invité.

ÉTAPE 6 Choisissez le VLAN que vous avez créé pour le réseau invité (ou, si vous n'avez pas encore créé de réseau, sélectionnez **Ajouter un VLAN**).

ÉTAPE 7 Cliquez sur **Enregistrer**. Le système vous indique que les ports Ethernet physiques sur le Cisco RV110W sont exclus du VLAN que vous avez attribué au réseau invité. En outre, l'isolation sans fil avec SSID et WMM est automatiquement activée.

Pour configurer le mot de passe et d'autres options :

ÉTAPE 1 Dans l'interface de gestion, choisissez **Sans fil** > **Paramètres de base**.

ÉTAPE 2 Sous la *Table sans fil*, cliquez sur **Modifier le réseau invité**.

ÉTAPE 3 Entrez un mot de passe que les utilisateurs devront fournir pour se connecter au réseau invité.

ÉTAPE 4 Ressaisissez le mot de passe pour le confirmer.

ÉTAPE 5 Entrez la durée, en minutes, pendant laquelle la connexion invitée sera disponible pour les utilisateurs.

ÉTAPE 6 (Facultatif) Pour restreindre l'utilisation de la bande passante par le réseau invité, cochez *Activer la restriction de bande passante invité*. (La qualité de service (QoS) doit d'abord être activée. Cliquez sur le lien vers la page Gestion de la bande passante si vous devez configurer la qualité de service.) Dans le champ *Bande passante disponible*, entrez le pourcentage de bande passante à allouer au réseau invité.

ÉTAPE 7 Cliquez sur **Enregistrer**.

Configuration des paramètres sans fil avancés

Les paramètres sans fil avancés sont réservés à un administrateur expert, car un mauvais réglage peut diminuer les performances sans fil.

Pour configurer les paramètres sans fil avancés :

ÉTAPE 1 Sélectionnez **Sans fil** > **Paramètres avancés**. La page Paramètres avancés apparaît.

ÉTAPE 2 Configurez les paramètres suivants :

Rafale de trames	Activez cette option pour accélérer les performances de vos réseaux sans fil, en fonction du fabricant de vos appareils réseau. Si vous n'êtes pas sûr de la manière d'exploiter cette option, conservez l'état par défaut (activé).

Aucune validation WMM	Cliquez pour activer cette fonctionnalité. L'activation de l'option Aucune validation WMM peut entraîner une amélioration du débit, mais aussi du taux d'erreurs dans un environnement hautes fréquences (RF) saturé. Cette option est désactivée par défaut.
Vitesse de base	Le paramètre Vitesse de base ne correspond pas à la vitesse de transmission, mais à une série de débits de transmission de la plateforme Services Ready Platform. Le Cisco RV110W annonce sa vitesse de base aux autres appareils sur le réseau, afin qu'ils connaissent les débits qui seront utilisés. La plateforme Services Ready Platform annonce également qu'elle sélectionnera automatiquement le meilleur débit de transmission. Le paramètre par défaut est Par défaut, lorsque le Cisco RV110W peut transmettre à tous les débits sans fil standard (1 Mbit/s, 2 Mbit/s, 5,5 Mbit/s, 11 Mbit/s, 18 Mbit/s, 24 Mbit/s, 36 Mbit/s, 48 Mbit/s et 54 Mbit/s). Le Cisco RV110W prend en charge les débits N en plus des débits B et G. L'option 1-2 Mbit/s sert aux anciennes technologies sans fil et l'option Tout lorsque le Cisco RV110W peut transmettre à toutes les vitesses sans fil. La vitesse de base ne correspond pas à la vitesse réelle de transmission des données. Si vous souhaitez spécifier la vitesse de transmission des données du Cisco RV110W, configurez le paramètre Vitesse de transmission.
Vitesse de transmission	Vous devez régler la vitesse de transmission en fonction de la vitesse de votre réseau sans fil. Faites un choix parmi différentes vitesses de transmission ou sélectionnez le mode automatique pour que le Cisco RV110W utilise la vitesse la plus rapide possible et la fonction de négociation automatique. La fonction de négociation automatique négocie la meilleure vitesse de connexion possible entre le Cisco RV110W et un client sans fil. La valeur par défaut est Automatique.

Vitesse de transmission N	Vous devez régler la vitesse de transmission en fonction de la vitesse de votre réseau sans fil de type N. Faites un choix parmi différentes vitesses de transmission ou sélectionnez le mode automatique pour que le Cisco RV110W utilise la vitesse la plus rapide possible et la fonction de négociation automatique. La fonction de négociation automatique négocie la meilleure vitesse de connexion possible entre le Cisco RV110W et un client sans fil. La valeur par défaut est Automatique.
Mode de protection CTS	Le Cisco RV110W utilise automatiquement le mode de protection CTS (Clear-To-Send) si vos appareils sans fil de type N et G rencontrent des problèmes et ne parviennent pas à transmettre vers le Cisco RV110W lorsque le trafic 802.11b environnant est très important. Cette fonction renforce la capacité du Cisco RV110W à capter les transmissions sans fil de type N et G, au prix d'une diminution considérable des performances. La valeur par défaut est Automatique.
Intervalle entre les signaux de balise	La valeur d'intervalle de balise indique la fréquence d'émission de la balise. Une balise est un paquet diffusé par le Cisco RV110W pour permettre la synchronisation du réseau sans fil. Entrez une valeur comprise entre 40 et 3500 millisecondes. La valeur par défaut est 100.
Intervalle DTIM	Cette valeur comprise entre 1 et 255 correspond à l'intervalle du message DTIM (Delivery Traffic Indication Message). Un champ DTIM est un champ de compte à rebours qui informe les clients de la prochaine fenêtre d'écoute des messages de diffusion et de multidiffusion. Lorsque les messages de diffusion ou de multidiffusion pour les clients associés sont stockés dans la mémoire tampon du Cisco RV110W, celui-ci envoie le message DTIM suivant avec une valeur d'intervalle DTIM. Les clients entendent les balises et sortent de veille pour recevoir les messages de diffusion ou de multidiffusion. La valeur par défaut est 1.

Seuil de fragmentation	Cette valeur spécifie la taille maximale d'un paquet au-delà de laquelle les données sont scindées en plusieurs paquets. Si vous rencontrez une quantité importante d'erreurs de paquets, essayez d'augmenter légèrement le seuil de fragmentation. Un réglage trop faible du seuil de fragmentation peut dégrader les performances du réseau. Seule une légère réduction de la valeur par défaut est recommandée. Dans la majorité des cas, conservez la valeur par défaut de 2346.
Seuil RTS	En cas de flux de données intermittent, essayez une réduction mineure. La valeur par défaut de 2347 est recommandée. Lorsque la taille d'un paquet réseau est inférieure au seuil RTS (Request to Send) prédéfini, le mécanisme RTS/CTS (Clear to Send) n'est pas enclenché. La plate-forme Services Ready Platform envoie des trames RTS à une station de réception et négocie l'envoi d'une trame de données. Après réception d'un RTS, la station sans fil répond par une trame CTS pour autoriser le début de la transmission.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration de WDS

Un WDS (Wireless Distribution System) est un système qui permet l'interconnexion sans fil de points d'accès sur un réseau. Il permet d'utiliser plusieurs points d'accès pour l'extension d'un réseau sans fil sans avoir recours à un réseau filaire pour les relier.

Pour établir un lien WDS, le Cisco RV110W ainsi que d'autres postes WDS doivent être configurés pour utiliser le même mode de réseau sans fil, canal sans fil, bande sans fil et types de chiffrement (aucun et WEP).

REMARQUE WDS est pris en charge sur un seul SSID.

Pour configurer un WDS :

ÉTAPE 1 Sélectionnez **Sans fil** > **WDS**.

ÉTAPE 2 Cochez la case **Autoriser la répétition du signal sans fil à l'aide d'un répéteur** pour activer le WDS.

ÉTAPE 3 Pour entrer manuellement l'adresse MAC d'un répéteur, cliquez sur le bouton **Manuel** ou choisissez **Automatique** pour que le routeur détecte automatiquement les points d'accès distants.

ÉTAPE 4 (Facultatif) Cliquez sur le bouton **Afficher l'analyse du site**.

La **Table des réseaux disponibles** apparaît et présente les points d'accès réseau disponibles.

a. (Facultatif) Cliquez sur le bouton **Actualiser** pour mettre à jour les entrées de la table.

b. Dans la **Table des réseaux disponibles**, sélectionnez jusqu'à trois points d'accès qui serviront de répéteurs.

c. Pour ajouter les adresses MAC des points d'accès sélectionnés aux champs MAC en dessous de la table, cliquez sur **Connexion**.

ÉTAPE 5 Si vous avez cliqué sur le bouton **Manuel**, entrez les adresses MAC de un à trois points d'accès qui serviront de répéteurs dans les champs **MAC 1**, **MAC 2** et **MAC 3**.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Configuration de WPS

Vous pouvez configurer le WPS (Wi-Fi Protected Setup) sur le Cisco RV110W pour permettre aux appareils compatibles WPS de se connecter plus facilement au réseau sans fil.

Pour configurer le WPS sur les appareils clients :

ÉTAPE 1 Sélectionnez **Sans fil** > **WPS**. La page Configuration Wi-Fi protégée apparaît.

ÉTAPE 2 Dans le menu déroulant **SSID**, sélectionnez le réseau sans fil sur lequel vous souhaitez activer le WPS.

ÉTAPE 3 Dans le champ **WPS**, cochez la case **Activer** pour activer le WPS. Décochez la case pour désactiver le WPS.

ÉTAPE 4 Configurez le WPS sur les appareils clients de l'une des trois manières suivantes :

- Méthode WPS 1
- Méthode WPS 2
- Méthode WPS 3

Une fois que vous avez configuré le WPS, les informations suivantes sont affichées au bas de la page **WPS** : État de la configuration Wi-Fi protégée, Nom du réseau (SSID), Sécurité, Chiffrement et Mot de passe.

Méthode WPS 1

Utilisez cette méthode si votre appareil client est doté d'un bouton WPS.

ÉTAPE 1 Cliquez ou appuyez sur le bouton WPS de l'appareil client.

ÉTAPE 2 Cliquez sur le bouton **WPS** de la page **WPS**. Une fois la configuration WPS terminée, une boîte de dialogue apparaît.

ÉTAPE 3 Cliquez sur **OK**.

Reportez-vous à la documentation de votre appareil client pour en savoir plus sur sa configuration.

Méthode WPS 2

Utilisez cette méthode si votre appareil client est doté d'un code PIN WPS.

ÉTAPE 1 Entrez le code PIN dans le champ de la page **WPS**.

ÉTAPE 2 Cliquez sur **Enregistrer**.

ÉTAPE 3 Une fois la configuration terminée, cliquez sur **OK**.

Reportez-vous à la documentation de votre appareil client pour en savoir plus sur sa configuration.

Méthode WPS 3

Si l'appareil client exige un code PIN du routeur, utilisez le numéro affiché sous le troisième élément de la page **WPS**.

4

Configuration du pare-feu

Ce chapitre présente la procédure à suivre pour configurer les propriétés de pare-feu du RV110W.

- **Fonctionnalités de pare-feu du Cisco RV110W**
- **Configuration des paramètres de base du pare-feu**
- **Gestion des horaires de pare-feu**
- **Configuration de la gestion de services**
- **Configuration des règles d'accès**
- **Création d'une stratégie d'accès à Internet**
- **Configuration de la redirection de ports**

Fonctionnalités de pare-feu du Cisco RV110W

Vous pouvez sécuriser votre réseau en créant et en appliquant des règles utilisées par le Cisco RV110W pour bloquer et autoriser du trafic Internet entrant et sortant. Vous spécifiez ensuite les appareils concernés par les règles. Pour ce faire, vous devez définir les éléments suivants :

- Services et types de trafic (exemples : navigation Web, VoIP, autres services standards et services personnalisés que vous définissez) que le routeur doit autoriser ou bloquer
- Direction du trafic en spécifiant la source et la destination du trafic avec la « zone source » (LAN/WAN/DMZ) et la « zone cible » (LAN/WAN/DMZ)
- Horaires d'application des règles par le routeur
- Mots clés (d'un nom de domaine ou d'une adresse URL d'une page Web) que le routeur doit autoriser ou bloquer

- Règles autorisant ou bloquant le trafic Internet entrant et sortant pour certains services à certaines heures
- Adresses MAC des appareils dont les accès entrants doivent être bloqués par le routeur
- Déclencheurs de ports qui indiquent au routeur d'autoriser ou de bloquer l'accès à certains services définis par leur numéro de port
- Rapports et alertes que vous souhaitez recevoir du routeur

Vous pouvez par exemple définir des règles d'accès restreint en fonction d'un horaire, d'une adresse Web ou de mots clés d'adresses Web. Vous pouvez bloquer l'accès Internet d'applications et de services sur le réseau local (LAN), comme les forums de discussion ou les jeux. Vous pouvez bloquer l'accès par le réseau étendu (WAN) ou la DMZ publique à certains groupes d'ordinateurs de votre réseau

Les règles entrantes (WAN vers LAN/DMZ) limitent l'accès du trafic entrant sur votre réseau, n'autorisant l'accès à certaines ressources locales qu'à certains utilisateurs externes. Par défaut, tous les accès au réseau LAN sécurisé provenant du réseau WAN non sécurisé sont bloqués, à l'exception des réponses aux requêtes provenant du LAN ou de la DMZ. Pour autoriser des appareils externes à accéder à des services sur le LAN sécurisé, vous devez définir une règle de pare-feu pour chaque service.

Si vous souhaitez autoriser le trafic entrant, l'adresse IP du port WAN du routeur doit être rendue publique. Cela s'appelle « exposer votre hôte ». La manière de rendre votre adresse publique dépend de la façon dont les ports WAN sont configurés. Sur le Cisco RV110W, vous pouvez utiliser l'adresse IP si une adresse statique est affectée au port WAN ou un nom DDNS (Dynamic DNS) si l'adresse de votre WAN est dynamique.

Les règles sortantes (LAN/DMZ vers WAN) limitent l'accès du trafic sortant de votre réseau, n'autorisant l'accès à certaines ressources externes qu'à certains utilisateurs locaux. La règle sortante par défaut est d'autoriser l'accès depuis la zone sécurisée (LAN) à la DMZ publique ou au WAN non sécurisé. Pour bloquer l'accès à Internet (WAN non sécurisé) par des hôtes du LAN sécurisé, vous devez créer une règle de pare-feu pour chaque service.

Configuration des paramètres de base du pare-feu

Pour configurer les paramètres de base du pare-feu :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Paramètres de base**.

ÉTAPE 2 Configurez les paramètres de pare-feu suivants :

Pare-feu	Cochez la case **Activer** pour pouvoir configurer les paramètres du pare-feu.
Protection DoS	Cochez la case **Activer** pour activer la protection contre les attaques de déni de service (DoS ou Denial of Service).
Bloquer la requête WAN	Bloque les requêtes Ping qui parviennent au Cisco RV110W depuis le WAN.
Accès Web	Sélectionnez le type d'accès Web autorisé pour la connexion au pare-feu : HTTP ou HTTPS (HTTP sécurisé).
Gestion à distance **Accès à distance** **Mise à niveau à distance** **Adresse IP distante autorisée** **Port de gestion à distance**	Reportez-vous à la section **Configuration de la gestion à distance**.
Intercommunication de multidiffusion IPv4 (proxy IGMP)	Cochez la case **Activer** pour activer l'intercommunication de multidiffusion pour IPv4.
Intercommunication de multidiffusion IPv6 (proxy IGMP)	Cochez la case **Activer** pour activer l'intercommunication de multidiffusion pour IPv6.

UPnP **Autoriser la configuration par les utilisateurs** **Autoriser les utilisateurs à désactiver l'accès à Internet**	Reportez-vous à la section **Configuration d'Universal Plug and Play**.
Bloquer Java	Cochez la case pour bloquer les applets Java. Les applets Java sont de petits programmes intégrés aux pages Web qui activent des fonctions dynamiques de la page. Un applet malveillant peut servir à compromettre ou infecter un ordinateur. Activez ce paramètre pour bloquer le téléchargement des applets Java. Cliquez sur **Automatique** pour bloquer Java automatiquement ou sur **Manuel** pour spécifier un port sur lequel Java doit être bloqué.
Bloquer les cookies	Cochez la case pour bloquer les cookies. Les sites Web utilisent les cookies pour stocker des informations de session. Toutefois, certains sites Web utilisent les cookies pour surveiller l'utilisateur et ses habitudes de navigation. Activez cette option pour empêcher la création de cookies par les sites Web. De nombreux sites Web ne sont pas accessibles lorsque les cookies sont refusés. Le blocage des cookies peut donc entraîner le dysfonctionnement de ces sites. Cliquez sur **Automatique** pour bloquer automatiquement les cookies ou sur **Manuel** pour spécifier un port sur lequel les cookies doivent être bloqués.

Bloquer ActiveX	Cochez la case pour bloquer le contenu ActiveX. Les contrôles ActiveX, similaires aux applets Java, sont installés sur les ordinateurs Windows qui utilisent Internet Explorer. Les contrôles ActiveX malveillants peuvent servir à compromettre ou infecter un ordinateur. Activez ce paramètre pour bloquer le téléchargement des contrôles ActiveX. Cliquez sur **Automatique** pour bloquer ActiveX automatiquement ou sur **Manuel** pour spécifier un port sur lequel ActiveX doit être bloqué.
Bloquer le proxy	Cochez la case pour bloquer les serveurs proxy. Un serveur mandataire ou proxy permet à un ordinateur d'acheminer les connexions aux autres ordinateurs par le biais du proxy, contournant ainsi certaines règles de pare-feu. Par exemple, lorsque les connexions à une adresse IP spécifique sont bloquées par une règle de pare-feu, ces requêtes peuvent être acheminées par le biais d'un proxy qui n'est pas bloqué par la règle, contournant ainsi la règle concernée. Activez cette option pour bloquer les serveurs proxy. Cliquez sur **Automatique** pour bloquer automatiquement les serveurs proxy ou sur **Manuel** pour spécifier un port sur lequel les serveurs proxy doivent être bloqués.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration de la gestion à distance

Activez la gestion à distance pour pouvoir accéder au Cisco RV110W à partir d'un réseau WAN distant.

Pour configurer la gestion à distance, configurez les règles suivantes sur la page **Paramètres de base** :

Gestion à distance	Cochez la case **Activer** pour activer la gestion à distance.
Accès à distance	Sélectionnez le type d'accès Web autorisé pour la connexion au pare-feu : HTTP ou HTTPS (HTTP sécurisé).
Mise à niveau à distance	Pour autoriser la mise à niveau à distance du Cisco RV110W, cochez la case **Activer**.
Adresse IP distante autorisée	Cliquez sur le bouton **Toute adresse IP** pour autoriser la gestion à distance à partir de toute adresse IP ou spécifiez une adresse IP spécifique dans le champ d'adresse.
Port de gestion à distance	Entrez le port sur lequel l'accès à distance est autorisé. Le port par défaut est 443. Lorsque vous accédez au routeur à distance, vous devez entrer le port de gestion à distance dans le cadre de l'adresse IP. Exemple : https://<*remote-ip*>:<*port_à_distance*> ou *https://168.10.1.11:443*

ATTENTION Lorsque la gestion à distance est activée, le routeur est accessible par tout utilisateur qui connaît l'adresse IP correspondante. Un utilisateur extérieur malveillant pouvant reconfigurer le Cisco RV110W, il est vivement conseillé de modifier le mot de passe administrateur et le mot de passe invité avant de continuer.

Configuration d'Universal Plug and Play

Universal Plug and Play (UPnP) permet la découverte automatique d'appareils capables de communiquer avec le Cisco RV110W.

Pour configurer l'UPnP, configurez les règles suivantes sur la page **Paramètres de base** :

UPnP	Cochez la case **Activer** pour activer le protocole UPnP.
Autoriser la configuration par les utilisateurs	Cochez cette case pour autoriser la définition de règles de correspondance de ports UPnP par les utilisateurs équipés d'ordinateurs ou d'autres appareils compatibles UPnP. Lorsque la case est décochée, le Cisco RV110W n'autorise pas les applications à ajouter des règles de transfert.
Autoriser les utilisateurs à désactiver l'accès à Internet	Cochez cette case pour autoriser les utilisateurs à désactiver l'accès à Internet.

Gestion des horaires de pare-feu

Vous pouvez créer des horaires afin d'appliquer les règles de pare-feu certains jours ou à certaines heures de la journée.

Ajout ou modification d'un horaire de pare-feu

Ajout ou modification d'un horaire de pare-feu

Pour créer ou modifier un horaire :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Gestion des horaires**.

ÉTAPE 2 Cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Dans le champ **Nom**, entrez un nom unique pour identifier l'horaire. Le nom est disponible dans la liste **Sélectionner un horaire** sur la page de configuration des règles de pare-feu. (Reportez-vous à la section **Configuration des règles d'accès**.)

ÉTAPE 4 Dans **Jours planifiés**, indiquez si vous souhaitez appliquer l'horaire à certains jours ou tous les jours. Si vous sélectionnez **Certains jours**, cochez les cases en regard des jours que vous souhaitez inclure dans l'horaire.

ÉTAPE 5 Dans **Heures planifiées**, sélectionnez la plage horaire d'application de l'horaire. Sélectionnez **Tout le temps** ou **À certaines heures**. Si vous choisissez **À certaines heures**, entrez l'heure de début et l'heure de fin.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Configuration de la gestion de services

Lorsque vous créez une règle de pare-feu, vous pouvez spécifier un service contrôlé par la règle. Différents types de services courants sont disponibles et vous pouvez aussi créer vos propres services.

La page **Gestion des services** permet de créer des services personnalisés auxquels les règles de pare-feu sont appliquées. Une fois défini, le nouveau service apparaît dans la table des **services personnalisés disponibles**.

Pour créer un service personnalisé :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Gestion des services**.

ÉTAPE 2 Cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Dans le champ **Nom du service**, entrez le nom du service pour pouvoir l'identifier plus tard.

ÉTAPE 4 Dans le champ **Protocole**, sélectionnez le protocole Layer 4 utilisé par le service dans le menu déroulant :

- **TCP**
- **UDP**
- **TCP et UDP**
- **ICMP**

ÉTAPE 5 Dans le champ **Port de début**, entrez le premier port TCP ou UDP de la plage utilisée par le service.

ÉTAPE 6 Dans le champ **Port de fin**, entrez le dernier port TCP ou UDP de la plage utilisée par le service.

ÉTAPE 7 Cliquez sur **Enregistrer**.

Pour modifier une entrée, sélectionnez-la et cliquez sur **Modifier**. Apportez les modifications voulues, puis cliquez sur **Enregistrer**.

Configuration des règles d'accès

Configuration de la stratégie appliquée par défaut au trafic sortant

La page **Règles d'accès** permet de configurer la stratégie sortante par défaut pour le trafic acheminé du réseau sécurisé (LAN) vers le réseau non sécurisé (WAN dédié/facultatif).

La stratégie entrante par défaut pour le trafic provenant de la zone non sécurisée en direction de la zone sécurisée est toujours bloquée et ne peut pas être modifiée.

Pour configurer la stratégie sortante par défaut :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Règles d'accès**.

ÉTAPE 2 Sélectionnez **Autoriser** ou **Refuser**.

Remarque : vérifiez que la prise en charge d'IPv6 est activée sur le Cisco RV110W pour configurer un pare-feu IPv6. Reportez-vous à la section **Configuration d'IPv6**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Réorganisation des règles d'accès

L'ordre dans lequel les règles d'accès sont affichées dans la table des règles d'accès indique l'ordre dans lequel elles sont appliquées. Vous pouvez réorganiser la table pour que certaines règles s'appliquent avant d'autres. Par exemple, si vous voulez appliquer une règle qui autorise certains types de trafic avant de bloquer d'autres types de trafic.

Pour réorganiser les règles d'accès :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Règles d'accès**.

ÉTAPE 2 Cliquez sur **Réorganiser**.

ÉTAPE 3 Cochez la case dans la ligne de la règle que vous souhaitez déplacer vers le haut ou le bas et cliquez sur la flèche vers le haut ou le bas pour déplacer la règle d'une ligne vers le haut ou vers le bas ou sélectionnez la position voulue de la règle dans la liste déroulante et cliquez sur **Déplacer vers**.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Ajout de règles d'accès

Toutes les règles de pare-feu configurées sur le Cisco RV110W sont affichées dans la **Table des règles d'accès**. Cette liste indique également si la règle est activée et présente les zones « source/cible » ainsi que les services et utilisateurs concernés par la règle.

Pour créer une règle d'accès :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Règles d'accès**.

ÉTAPE 2 Cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Dans le champ **Type de connexion**, sélectionnez la direction du trafic :

- **Sortant (LAN > WAN)** : sélectionnez cette option pour créer une règle sortante.
- **Entrant (WAN > LAN)** : sélectionnez cette option pour créer une règle entrante.
- **Entrant (WAN > DMZ)** : sélectionnez cette option pour créer une règle entrante.

ÉTAPE 4 Sélectionnez une action dans le menu déroulant **Action** :

- **Toujours bloquer** : toujours bloquer le type de trafic sélectionné.
- **Toujours autoriser** : ne jamais bloquer le type de trafic sélectionné.

- **Bloquer selon l'horaire, sinon autoriser** : bloque le type de trafic sélectionné en fonction d'une planification spécifique.
- **Autoriser selon l'horaire, sinon bloquer** : autorise le type de trafic sélectionné en fonction d'une planification spécifique.

ÉTAPE 5 Dans le menu déroulant **Services**, sélectionnez le service à autoriser ou bloquer pour cette règle. Sélectionnez **Tout le trafic** pour appliquer la règle à tous les services et applications ou sélectionnez une application particulière à bloquer :

- DNS (Domain Name System), UDP ou TCP
- FTP (File Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- TFTP (Trivia File Transfer Protocol)
- IMAP (Internet Message Access Protocol)
- NNTP (Network News Transport Protocol)
- POP3 (Post Office Protocol)
- SNMP (Simple Network Management Protocol)
- SMTP (Simple Mail Transfer Protocol)
- Telnet
- STRMWORKS
- TACACS (Terminal Access Controller Access-Control System)
- Telnet (commande)
- Telnet secondaire
- Telnet SSL
- Voix (SIP)

ÉTAPE 6 (Facultatif) Cliquez sur **Configurer les services** pour aller sur la page **Gestion de services** afin de définir les services avant de leur appliquer des règles d'accès.

Pour plus d'informations, reportez-vous à la section **Configuration de la gestion de services**.

ÉTAPE 7 Dans le champ **IP source**, sélectionnez les utilisateurs auxquels appliquer la règle :

- **Tout** : la règle s'applique au trafic provenant de tout hôte du réseau local.
- **Adresse individuelle** : la règle s'applique au trafic provenant d'une adresse IP spécifique du réseau local. Saisissez l'adresse dans le champ **Début**.
- **Plage d'adresses** : la règle s'applique au trafic provenant d'une adresse IP appartenant à une plage d'adresses spécifique. Saisissez l'adresse IP de début dans le champ **Début** et l'adresse IP de fin dans le champ **Fin**.

ÉTAPE 8 Dans le champ **Journal**, spécifiez si les paquets correspondant à cette règle doivent être consignés dans un journal.

Pour consigner les détails de tous les paquets correspondants à la règle, sélectionnez **Toujours** dans le menu déroulant. Exemple : si une règle sortante pour un horaire est réglée sur **Toujours bloquer**, à chaque fois qu'un paquet tente d'établir une connexion sortante pour le service concerné, un message contenant l'adresse source et de destination du paquet (ainsi que d'autres informations) est enregistré dans le journal.

L'activation de la journalisation peut engendrer un volume conséquent de messages de journal et n'est recommandée qu'à des fins de débogage.

Sélectionnez **Jamais** pour désactiver la journalisation.

Remarque : lorsque le trafic va du LAN ou de la DMZ vers le WAN, le système exige la réécriture de l'adresse IP source ou de destination des paquets IP entrants lorsqu'ils transitent par le pare-feu.

ÉTAPE 9 Dans le champ **Priorité QoS**, affectez une priorité aux paquets IP du service. Les priorités sont définies par niveau de QoS : (**1 (minimum)**, **2**, **3**, **4 (maximum)**).

ÉTAPE 10 Dans le champ **État de la règle**, cochez la case pour activer la nouvelle règle d'accès.

ÉTAPE 11 Cliquez sur **Enregistrer**.

Création d'une stratégie d'accès à Internet

Le Cisco RV110W prend en charge plusieurs options permettant de bloquer l'accès à Internet. Vous pouvez bloquer l'ensemble du trafic Internet, le bloquer au niveau de certains ordinateurs ou points de terminaison ou encore bloquer l'accès à des sites Internet en spécifiant des mots clés spécifiques. Si ces mots clés sont détectés dans le nom d'un site (URL du site, nom d'un newsgroup, etc.), le site est bloqué.

Ajout ou modification d'une stratégie d'accès à Internet

Pour créer une politique d'accès à Internet :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Stratégie d'accès à Internet**.

ÉTAPE 2 Cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Dans le champ **État**, cochez la case **Activer**.

ÉTAPE 4 Entrez un nom de stratégie pour pouvoir l'identifier plus tard.

ÉTAPE 5 Dans le menu déroulant **Action**, sélectionnez le type de restriction d'accès voulu :

- **Toujours bloquer** : toujours bloquer le trafic Internet. Cette option bloque le trafic Internet en provenance et en direction de tous les points de terminaison. Si vous souhaitez bloquer l'intégralité du trafic, mais autoriser certains points de terminaison à recevoir du trafic Internet, reportez-vous à l'étape 7.
- **Toujours autoriser** : toujours autoriser le trafic Internet. Vous pouvez affiner ce paramètre afin de bloquer certains points de terminaison spécifiés du trafic Internet. Pour cela, reportez-vous à l'étape 7. Vous pouvez également autoriser l'ensemble du trafic Internet à l'exception de certains sites Web ; reportez-vous à l'étape 8.
- **Bloquer selon l'horaire** : bloque le trafic Internet selon un horaire précis (par exemple, si vous souhaitez bloquer le trafic Internet pendant les heures de travail, mais l'autoriser après les heures de travail et pendant le week-end).
- **Autoriser selon l'horaire** : autorise le trafic Internet en fonction d'un horaire.

Si vous sélectionnez **Bloquer selon l'horaire** ou **Autoriser selon l'horaire**, cliquez sur **Configurer les horaires** pour créer un horaire. Reportez-vous à la section **Gestion des horaires de pare-feu**.

ÉTAPE 6 Sélectionnez un horaire dans le menu déroulant.

ÉTAPE 7 (Facultatif) Appliquez la stratégie d'accès à des ordinateurs particuliers afin d'autoriser ou de bloquer le trafic provenant de périphériques particuliers :

a. Dans la table **Appliquer la stratégie d'accès aux ordinateurs suivants**, cliquez sur **Ajouter une ligne**.

b. Dans le menu déroulant **Type**, sélectionnez la manière d'identifier l'ordinateur (adresse MAC, adresse IP ou plage d'adresses IP).

c. En fonction du choix effectué à l'étape précédente, entrez l'une des valeurs suivantes dans le champ **Valeur** :

- L'adresse MAC (xx:xx:xx:xx:xx:xx) de l'ordinateur ciblé par la stratégie
- L'adresse IP des ordinateurs ciblés par la stratégie
- Les adresses IP de début et de fin de la plage d'adresses à bloquer (comme 192.168.1.2-192.168.1.253)

ÉTAPE 8 Pour bloquer le trafic de sites Web particuliers :

a. Dans la table **Blocage de site Web**, cliquez sur **Ajouter une ligne**.

b. Dans le menu déroulant **Type**, sélectionnez la manière de bloquer le site web (en spécifiant l'URL ou un mot clé qui est inclus dans l'URL).

c. Dans le champ **Valeur**, entrez l'URL ou mot clé de blocage du site Web.

Exemple : pour bloquer l'URL exemple.com, sélectionnez **Adresse URL** dans le menu déroulant, puis entrez **exemple.com** dans le champ **Valeur**. Pour bloquer une URL qui contient le mot clé « exemple », sélectionnez **Mot clé** dans le menu déroulant et entrez **exemple** dans le champ **Valeur**.

ÉTAPE 9 Cliquez sur **Enregistrer**.

Configuration de la redirection de ports

La redirection de ports sert à rediriger le trafic Internet d'un port du réseau WAN vers un autre port du réseau LAN. Des services courants sont disponibles, mais vous pouvez également définir un service personnalisé et les ports associés pour la redirection.

Les pages **Redirection de ports individuels** et **Redirection de plages de ports** présentent toutes les règles de redirection de ports de l'appareil et vous permettent de les configurer.

REMARQUE La redirection de port ne s'applique pas aux serveurs du LAN, en raison de la dépendance entre l'appareil LAN qui établit une connexion sortante avant l'ouverture des ports entrants.

Pour fonctionner correctement, certaines applications doivent recevoir des données sur un port particulier ou une plage de ports particulière lorsque des appareils externes s'y connectent. Le routeur doit envoyer toutes les données entrantes pour cette application uniquement au port ou à la plage de ports spécifiques.

La passerelle dispose d'une liste d'applications et de jeux avec des ports entrants et sortants associés à ouvrir. Vous pouvez également spécifier une règle de redirection de port en spécifiant le type de trafic (TCP ou UDP) et la plage de ports entrants et sortants à ouvrir.

Configuration de la redirection de port individuel

Pour ajouter une règle de redirection de port individuel :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Redirection de port individuel**. Une liste d'applications prédéfinies est affichée.

ÉTAPE 2 Dans le champ **Application**, entrez le nom de l'application pour laquelle vous souhaitez configurer la redirection de port.

ÉTAPE 3 Dans le champ **Port externe**, entrez le numéro de port qui déclenche la règle en cas de demande de connexion émise par le trafic sortant.

ÉTAPE 4 Dans le champ **Port interne**, entrez le numéro de port utilisé par l'appareil distant pour répondre à la demande qu'il reçoit.

ÉTAPE 5 Dans le menu déroulant **Protocole**, sélectionnez un protocole (**TCP**, **UDP** ou **TCP** et **UDP**).

ÉTAPE 6 Dans le champ **Adresse IP**, entrez l'adresse IP de l'hôte, côté LAN, vers laquelle le trafic IP spécifique doit être redirigé. Par exemple, vous pouvez rediriger le trafic http vers le port 80 de l'adresse IP d'un serveur Web côté LAN.

ÉTAPE 7 Cochez la case **Activer** dans le champ correspondant pour activer la règle.

ÉTAPE 8 Cliquez sur **Enregistrer**.

Configuration de la redirection d'une plage de ports

Pour ajouter une règle de redirection de plage de ports :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Redirection de plage de ports**.

ÉTAPE 2 Dans le champ **Application**, entrez le nom de l'application pour laquelle vous souhaitez configurer la redirection de port.

ÉTAPE 3 Dans le champ **Port externe**, entrez le numéro de port qui déclenche la règle en cas de demande de connexion émise par le trafic sortant.

ÉTAPE 4 Dans le champ **Début**, indiquez le numéro de port de début de la plage de ports à rediriger.

ÉTAPE 5 Dans le champ **Fin**, indiquez le numéro de port de fin de la plage de ports à rediriger.

ÉTAPE 6 Dans le menu déroulant **Protocole**, sélectionnez un protocole (**TCP**, **UDP** ou **TCP** et **UDP**).

ÉTAPE 7 Dans le champ **Adresse IP**, entrez l'adresse IP de l'hôte, côté LAN, vers laquelle le trafic IP spécifique doit être redirigé.

ÉTAPE 8 Cochez la case **Activer** dans le champ correspondant pour activer la règle.

ÉTAPE 9 Cliquez sur **Enregistrer**.

Configuration du déclenchement de plage de ports

Le déclenchement de plages de ports permet aux appareils du LAN ou de la DMZ de demander qu'un ou plusieurs ports soient redirigés vers eux. Le mécanisme de déclenchement de port attend une demande sortante du LAN/DMZ sur l'un des ports sortants définis, puis ouvre un port entrant pour le type de trafic concerné.

Le déclenchement des ports est une forme de redirection de ports dynamiques lorsqu'une application transmet des données sur les ports entrants et sortants ouverts. Il ouvre un port entrant pour un type de trafic particulier sur un port sortant défini. Cette option est plus souple que la redirection de port statique (disponible lors de la configuration de règles de pare-feu), car il n'est pas nécessaire que la règle cible une adresse IP ni une plage IP du réseau LAN. En outre, les ports sont fermés lorsqu'ils ne sont pas utilisés, offrant ainsi un niveau de sécurité supérieur à la redirection de ports.

REMARQUE La redirection de port ne s'applique pas aux serveurs du LAN, en raison de la dépendance sur l'appareil LAN qui établit une connexion sortante avant l'ouverture des ports entrants.

Pour fonctionner correctement, certaines applications doivent recevoir des données sur un port particulier ou une plage de ports particulière lorsque des appareils externes s'y connectent. Le routeur doit envoyer toutes les données entrantes pour cette application uniquement au port ou à la plage de ports spécifiques. La passerelle dispose d'une liste d'applications et de jeux avec des ports entrants et sortants associés à ouvrir. Vous pouvez également spécifier une règle de déclenchement de ports en spécifiant le type de trafic (TCP ou UDP) et la plage de ports entrants et sortants à ouvrir.

Pour ajouter une règle de déclenchement de port :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Déclenchement de plage de ports**.

ÉTAPE 2 Dans le champ **Application**, entrez le nom de l'application pour laquelle vous souhaitez configurer la redirection de port.

ÉTAPE 3 Dans le champ **Plage déclenchée**, entrez le numéro de port ou la plage de numéros de ports qui déclenche la règle en cas de demande de connexion émise par le trafic sortant. Si la connexion sortante n'utilise qu'un seul port, entrez le même numéro de port dans les deux champs.

ÉTAPE 4 Dans les champs **Plage redirigée**, entrez le numéro de port ou les numéros de plage de ports utilisés par le système distant pour répondre à la demande qu'il reçoit. Si la connexion entrante n'utilise qu'un seul port, entrez le même numéro de port dans les deux champs.

ÉTAPE 5 Cochez la case **Activer** dans le champ correspondant pour activer la règle.

ÉTAPE 6 Cliquez sur **Enregistrer**.

5

Configuration de VPN

Ce chapitre explique comment configurer le VPN et la sécurité pour le Cisco RV110W.

- **Types de tunnels VPN, page 100**
- **Clients VPN, page 101**
- **Configuration de la gestion des certificats, page 113**
- **Configuration de l'intercommunication VPN, page 115**

Types de tunnels VPN

Les VPN offrent un canal de communication sécurisé (« tunnel ») entre deux routeurs-passerelles ou entre un télétravailleur et un routeur-passerelle. Vous pouvez créer différents types de tunnels VPN en fonction des besoins de votre entreprise. Différents exemples sont proposés ci-dessous. Lisez ces descriptions afin de comprendre les diverses options et les procédures requises pour configurer votre VPN.

Accès distant via PPTP

Dans cet exemple, un utilisateur distant équipé d'un ordinateur Microsoft se connecte à un serveur PPTP sur votre site, afin d'accéder aux ressources du réseau. Utilisez cette option pour simplifier la configuration VPN. Vous n'avez pas à configurer de stratégies VPN. Les utilisateurs distants peuvent se connecter à l'aide du client PPTP à partir d'un ordinateur Microsoft. Vous n'avez pas à installer de client VPN. Toutefois, tenez compte du fait que des vulnérabilités en matière de sécurité ont été détectées dans ce protocole.

Entrez les paramètres du serveur PPTP et ajoutez les utilisateurs sur la page *VPN > Clients VPN*, dans la table des paramètres des clients VPN. Choisissez PPTP en tant que protocole utilisateur. Reportez-vous à la section **Création et gestion des utilisateurs PPTP**.

Accès distant avec Cisco QuickVPN

Pour définir rapidement les paramètres de sécurité VPN de base, distribuez le logiciel Cisco QuickVPN à vos utilisateurs, qui pourront alors accéder à vos ressources réseau de manière sécurisée. Utilisez cette option si vous souhaitez simplifier le processus de configuration VPN. Vous n'avez pas à configurer de stratégies VPN. Les utilisateurs distants peuvent se connecter de manière sécurisée à l'aide du client Cisco QuickVPN et d'une connexion Internet.

1. Ajoutez les utilisateurs sur la page *VPN > Clients VPN*, dans la table des paramètres des clients VPN. Choisissez QuickVPN en tant que protocole utilisateur. Reportez-vous à la section **Importation des paramètres client VPN**.
2. Demandez aux utilisateurs de récupérer le logiciel gratuit Cisco QuickVPN sur le site Cisco.com et de l'installer sur leurs ordinateurs. Pour plus d'informations, reportez-vous au **Annexe A, « Utilisation de Cisco QuickVPN ».**

Pour activer l'accès via Cisco QuickVPN sur ce routeur, vous devez activer la gestion à distance afin d'ouvrir le port 443 pour SSL. Reportez-vous à la section **Configuration des paramètres de base du pare-feu**.

VPN site-à-site

Le Cisco RV110W prend en charge le VPN site-à-site pour un tunnel VPN passerelle-à-passerelle unique. Par exemple, vous pouvez configurer le Cisco RV110W sur un site de filiale pour qu'il se connecte au routeur du site de l'entreprise, afin que le site de la filiale puisse accéder en toute sécurité au réseau de l'entreprise. La configuration du VPN site-à-site s'effectue sur la page **VPN** > **Configuration VPN de base**.

Clients VPN

Le logiciel client VPN est nécessaire pour établir un tunnel VPN entre le routeur et le point d'extrémité distant. Les logiciels open source (tels qu'OpenVPN ou Openswan) et les logiciels VPN IPsec Microsoft peuvent être configurés pour établir un tunnel VPN IPsec. Reportez-vous au guide d'utilisation du logiciel client et à l'aide en ligne du routeur pour obtenir des instructions détaillées sur la configuration.

Configuration du protocole PPTP

Le protocole PPTP (Point to Point Tunneling Protocol) est un protocole réseau permettant de transférer en toute sécurité des données depuis un client distant vers un réseau d'entreprise en créant une connexion VPN sécurisée sur les réseaux publics, comme Internet.

REMARQUE Lors de l'activation du VPN sur le Cisco RV110W, le sous-réseau LAN sur le Cisco RV110W est automatiquement modifié pour éviter les conflits d'adresses IP entre le réseau distant et le réseau local.

Pour configurer le service VPN PPTP :

ÉTAPE 1 Sélectionnez **VPN** > **Clients VPN**.

ÉTAPE 2 Procédez comme suit :

Serveur PPTP	Cochez cette case pour activer le serveur PPTP.
Adresse IP du serveur PPTP	Saisissez l'adresse IP du serveur PPTP.
Adresses IP des clients PPTP	Saisissez la plage d'adresses IP des clients PPTP.
Chiffrement MPPE	Cochez la case **Activer** pour activer le chiffrement MPPE. Le chiffrement MPPE (Microsoft Point-to-Point Encryption) est utilisé lorsque les utilisateurs configurent et emploient un client VPN PPTP pour se connecter au Cisco RV110W.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration de NetBIOS sur VPN

Pour activer NetBIOS sur VPN :

ÉTAPE 1 Dans le champ **NetBIOS sur VPN**, cochez la case pour permettre aux diffusions NetBIOS de traverser le tunnel VPN. Par défaut, la fonction NetBIOS est disponible pour les stratégies client.

ÉTAPE 2 Cliquez sur **Enregistrer**.

Création et gestion des utilisateurs PPTP

Pour créer des utilisateurs PPTP :

ÉTAPE 1 Dans la **Table des paramètres des clients VPN**, cliquez sur **Ajouter une ligne**.

ÉTAPE 2 Saisissez les informations suivantes :

Activer	Cochez cette case pour activer l'utilisateur.
Nom d'utilisateur	Saisissez le nom d'utilisateur de l'utilisateur PPTP (entre 4 et 32 caractères).
Mot de passe	Saisissez le mot de passe (entre 4 et 32 caractères).
Protocole	Sélectionnez **PPTP** dans le menu déroulant.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Pour modifier les paramètres d'un utilisateur PPTP, cochez la case correspondante, puis cliquez sur **Modifier**. Une fois que vous avez terminé, cliquez sur **Enregistrer**.

Pour supprimer un utilisateur PPTP, cochez la case correspondante, puis cliquez sur **Supprimer**.

Création et gestion des utilisateurs QuickVPN

Pour créer des utilisateurs QuickVPN :

ÉTAPE 1 Dans la **Table des paramètres des clients VPN**, cliquez sur **Ajouter une ligne**.

ÉTAPE 2 Saisissez les informations suivantes :

Activer	Cochez cette case pour activer l'utilisateur.
Nom d'utilisateur	Saisissez le nom d'utilisateur de l'utilisateur QuickVPN (entre 4 et 32 caractères).
Mot de passe	Saisissez le mot de passe (entre 4 et 32 caractères).
Autoriser l'utilisateur à modifier le mot de passe	Cochez cette case pour autoriser l'utilisateur à modifier le mot de passe.
Protocole	Sélectionnez **QuickVPN** dans le menu déroulant.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Pour modifier les paramètres d'un utilisateur QuickVPN, cochez la case correspondante, puis cliquez sur **Modifier**. Une fois les modifications terminées, cliquez sur **Enregistrer**.

Pour supprimer un utilisateur QuickVPN, cochez la case correspondante, puis cliquez sur **Supprimer**. Cliquez ensuite sur **Enregistrer**.

Pour plus d'informations sur QuickVPN, reportez-vous à l'**Annexe A, « Utilisation de Cisco QuickVPN ».**

Importation des paramètres client VPN

Vous pouvez importer des fichiers de paramètres client VPN contenant le nom d'utilisateur et le mot de passe des clients dans un fichier CSV (Comma Separated Value).

Vous pouvez utiliser un programme tel que Microsoft Excel pour créer un fichier CSV contenant les paramètres client VPN. Ce fichier doit contenir une ligne pour les en-têtes et une ou plusieurs lignes pour les clients VPN.

L'exemple suivant spécifie les paramètres de deux utilisateurs (un utilisateur PPTP et un utilisateur QuickVPN) à importer :

PROTOCOLE	NOM D'UTILISATEUR	MOT DE PASSE
PPTP	pptp-user-1	12345678
QuickVPN	qv-user-1	12345678

ATTENTION L'importation de paramètres client VPN entraîne la suppression des paramètres existants.

Pour importer des paramètres client VPN :

ÉTAPE 1 Cliquez sur **Parcourir** pour trouver le fichier.

ÉTAPE 2 Cliquez sur **Importer** pour charger le fichier.

ÉTAPE 3 À l'invite, pour supprimer les paramètres d'utilisateur VPN existants et importer les paramètres du fichier CSV, cliquez sur **Oui**.

Configuration des paramètres VPN de base (VPN site-à-site)

Le Cisco RV110W prend en charge le VPN site-à-site pour un tunnel VPN passerelle-à-passerelle unique. Dans cette configuration, le Cisco RV110W crée une connexion sécurisée vers un autre routeur VPN. Par exemple, vous pouvez configurer le Cisco RV110W sur un site de filiale pour qu'il se connecte au routeur du site de l'entreprise, afin que le site de la filiale puisse accéder en toute sécurité au réseau de l'entreprise. Vous pouvez par exemple prévoir un routeur comme le Cisco RV220W qui prend en charge dix tunnels VPN site-à-site et prévoir un Cisco RV110W sur chaque site distant pour assurer la sécurité des connexions.

Pour configurer les paramètres VPN de base pour une connexion site-à-site :

ÉTAPE 1 Sélectionnez **VPN** > **Configuration VPN de base**.

ÉTAPE 2 Dans le champ **Nom de la connexion**, entrez le nom du tunnel VPN.

ÉTAPE 3 Dans le champ **Clé pré-partagée**, entrez la clé pré-partagée, ou le mot de passe, qui sera échangée entre les deux routeurs. La clé pré-partagée doit comporter entre 8 et 49 caractères.

ÉTAPE 4 Dans les champs **Informations sur le point d'extrémité**, entrez les informations suivantes :

- **Point d'extrémité distant** : choisissez le moyen d'identifier le point d'extrémité distant ou le routeur auquel le Cisco RV110W se connectera (par adresse IP, par exemple, *192.168.1.1* ou par nom de domaine complet, par exemple, *cisco.com*).
- **Adresse IP de WAN (Internet) distant** : entrez l'adresse IP publique ou le nom de domaine du point d'extrémité distant.
- **Adresse IP de WAN (Internet) local** : entrez l'adresse IP publique ou le nom de domaine du point d'extrémité local (Cisco RV110W).

ÉTAPE 5 Dans les champs **Accessibilité distante par connexion sécurisée**, entrez les informations suivantes :

- **Adresse IP du réseau local (LAN) distant** : entrez l'adresse de réseau privé (LAN) du point d'extrémité distant. Il s'agit de l'adresse IP du réseau interne pour le site distant.
- **Masque de sous-réseau du réseau local (LAN) distant** : entrez le masque de sous-réseau du réseau privé (LAN) du point d'extrémité distant.
- **Adresse IP du réseau local (LAN)** : entrez l'adresse de réseau privé (LAN) du réseau local. Il s'agit de l'adresse IP du réseau interne sur le Cisco RV110W.
- **Masque de sous-réseau du réseau local (LAN)** : entrez le masque de sous-réseau du réseau privé (LAN) du réseau local (Cisco RV110W).

Remarque : Les adresses IP de WAN distant et de LAN distant ne peuvent pas exister sur le même sous-réseau. Par exemple, l'adresse IP de LAN distant 192.168.1.100 et l'adresse IP de LAN local 192.168.1.115 risquent de créer un conflit lorsque le trafic est acheminé via le VPN. Le troisième octet doit être différent pour que les adresses IP soient sur des sous-réseaux différents. Par exemple, l'adresse IP de LAN distant 192.168.1.100 et l'adresse IP de LAN local 192.168.2.100 sont acceptées.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Affichage des valeurs par défaut

Les valeurs par défaut utilisées dans les paramètres VPN de base sont celles proposées par le VPN Consortium et elles supposent que vous utilisez une clé pré-partagée, ou un mot de passe, connue du Cisco RV110W et du routeur à l'autre extrémité (par exemple, un Cisco RV220W). Pour afficher les valeurs par défaut :

ÉTAPE 1 Sélectionnez **VPN** > **Configuration VPN de base**.

ÉTAPE 2 Cliquez sur **Afficher les paramètres par défaut** pour afficher les valeurs par défaut.

Pour plus d'informations sur ces valeurs, reportez-vous à la section **Configuration des paramètres VPN avancés**.

Configuration des paramètres VPN avancés

La page *Configuration VPN avancée* vous permet de configurer les paramètres VPN avancés, tels que les stratégies IKE et d'autres stratégies VPN. Ces stratégies déterminent la façon dont le Cisco RV110W initie et reçoit les connexions VPN avec d'autres points d'extrémité.

Gestion des stratégies IKE

Gestion des stratégies IKE

Le protocole IKE (Internet Key Exchange) échange des clés entre deux hôtes IPsec de manière dynamique. Vous pouvez créer des stratégies IKE pour définir des paramètres de sécurité, tels que l'authentification de l'homologue ou les algorithmes de chiffrement à utiliser dans ce processus. Veillez à utiliser des paramètres de chiffrement, d'authentification et de clé-groupe compatibles dans la stratégie VPN.

Pour gérer les stratégies IKE :

ÉTAPE 1 Sélectionnez **VPN** > **IPsec** > **Configuration VPN avancée**.

ÉTAPE 2 Dans la **table des stratégies IKE**, cochez la case dans la ligne de la connexion VPN pour effectuer les tâches suivantes :

- **Modifier** : permet de modifier les propriétés de la stratégie IKE. Reportez-vous à la section **Ajout ou modification de stratégies IKE**.

- **Activer** : permet d'activer la stratégie.
- **Désactiver** : permet de désactiver la stratégie.
- **Supprimer** : permet de supprimer la stratégie. (**Remarque :** vous ne pouvez pas supprimer une stratégie IKE si elle est utilisée dans une stratégie VPN. Vous devez d'abord désactiver et supprimer la stratégie VPN dans la table des **stratégies VPN**.)
- **Ajouter une ligne** : permet d'ajouter une stratégie IKE. Reportez-vous à la section **Ajout ou modification de stratégies IKE**. (**Remarque** : si une connexion VPN est déjà configurée, vous devez la supprimer pour ajouter une autre connexion.)

ÉTAPE 3 Cliquez sur **Enregistrer**.

Gestion des stratégies VPN

Gestion des stratégies VPN

Pour gérer les stratégies VPN :

ÉTAPE 1 Sélectionnez **VPN** > **IPsec** > **Configuration VPN avancée**.

ÉTAPE 2 Dans la **table des stratégies VPN**, cochez la case dans la ligne de la connexion VPN pour effectuer les tâches suivantes :

- **Modifier** : permet de modifier les propriétés de la stratégie VPN. Reportez-vous à la section **Ajout ou modification de stratégies VPN**.
- **Activer** : permet d'activer la stratégie.
- **Désactiver** : permet de désactiver la stratégie.
- **Supprimer** : permet de supprimer la stratégie.
- **Ajouter une ligne** : permet d'ajouter une stratégie VPN. Reportez-vous à la section **Ajout ou modification de stratégies VPN**. (**Remarque** : si une connexion VPN est déjà configurée, vous devez la supprimer pour ajouter une autre connexion.)

ÉTAPE 3 Cliquez sur **Enregistrer**.

Ajout ou modification de stratégies IKE

Pour ajouter ou modifier des stratégies IKE, configurez les paramètres suivants :

- **Nom de la stratégie** : saisissez un nom unique à attribuer à la stratégie à des fins d'identification et de gestion.
- **Mode Exchange** : choisissez l'une des options suivantes :
  - **Principal** : ce mode négocie le tunnel avec une sécurité supérieure, mais est plus lent.
  - **Agressif** : ce mode établit plus rapidement la connexion, mais la sécurité est inférieure.

Dans la section *Paramètres de SA IKE*, les paramètres d'association de sécurité (SA) définissent la robustesse et le mode de négociation de l'association de sécurité. Vous pouvez configurer les paramètres suivants :

- **Algorithme de chiffrement** : choisissez l'algorithme utilisé pour négocier l'association de sécurité :
  - **DES**
  - **3DES**
  - **AES-128**
  - **AES-192**
  - **AES-256**
- **Algorithme d'authentification** : spécifiez l'algorithme d'authentification de l'en-tête VPN :
  - **MD5**
  - **SHA-1**
  - **SHA2-256**

    Veillez à ce que l'algorithme d'authentification soit configuré de façon identique des deux côtés du tunnel VPN (par exemple, sur le Cisco RV110W et sur le routeur auquel il se connecte).
- **Clé pré-partagée** : entrez la clé dans l'espace prévu à cet effet. Veuillez noter que les guillemets anglais (") ne sont pas pris en charge dans la clé prépartagée.

- **Groupe Diffie-Hellman (DH)** : spécifiez l'algorithme de groupe DH qui est utilisé lors de l'échange de clés. Le groupe DH définit la robustesse de l'algorithme, en bits. Vérifiez que le groupe DH est configuré de manière identique des deux côtés de la stratégie IKE.
- **Durée de vie SA** : saisissez l'intervalle, en secondes, au bout duquel l'association de sécurité devient non valide.
- **Détection d'homologue indisponible** : cochez la case **Activer** pour activer cette fonction ou décochez la case pour la désactiver. La détection d'homologue indisponible sert à détecter si l'homologue est actif ou non. Si l'homologue est détecté comme étant indisponible, le routeur supprime l'association de sécurité IPsec et l'association de sécurité IKE. Si vous activez cette fonction, entrez également les paramètres suivants :
  - **Action DPD** : entrez l'intervalle, en secondes, entre les messages DPD R-U-THERE consécutifs. Les messages DPD R-U-THERE sont envoyés uniquement lorsque le trafic IPsec est inactif.
  - **Expiration DPD** : indiquez combien de temps le Cisco RV110W doit attendre pour recevoir une réponse au message DPD avant de considérer l'homologue comme inactif.

Ajout ou modification de stratégies VPN

Pour créer une stratégie VPN automatique, vous devez d'abord créer une stratégie IKE, puis ajouter la stratégie automatique correspondant à cette stratégie IKE.

Pour ajouter ou modifier des stratégies VPN, configurez les paramètres suivants:

- **Nom de la stratégie** : saisissez un nom unique permettant d'identifier la stratégie.
- **Type de stratégie** : choisissez l'une des options suivantes :
  - **Stratégie automatique** : certains paramètres du tunnel VPN sont générés automatiquement. Cette option nécessite l'utilisation du protocole IKE (Internet Key Exchange) pour les négociations entre les deux points d'extrémité VPN.
  - **Stratégie manuelle** : tous les paramètres (y compris les clés) du tunnel VPN sont saisis manuellement pour chaque point d'extrémité. Aucun serveur tiers ni aucune organisation tierce n'est impliqué(e).
- **Point d'extrémité distant** : sélectionnez le type d'identifiant de passerelle à fournir sur le point d'extrémité distant : **Adresse IP** ou **FQDN** (nom de domaine complet). Entrez ensuite l'identifiant dans la zone prévue à cet effet.

Dans *Sélection de trafic en local* et *Sélection de trafic distant*, entrez les paramètres suivants :

- **Adresse IP locale/Adresse IP distante** : sélectionnez le type d'identifiant que vous souhaitez fournir pour le point d'extrémité :
  - **Individuelle** : limite la stratégie à un seul hôte. Dans le champ Adresse IP de début, saisissez l'adresse IP de l'hôte qui fera partie du VPN. Entrez ensuite la même adresse IP dans le champ **Adresse de début**.
  - **Sous-réseau** : autorise l'ensemble d'un sous-réseau à se connecter au VPN. Saisissez l'adresse de réseau dans le champ Adresse IP de début et saisissez le masque de sous-réseau dans le champ Masque de sous-réseau. Entrez l'adresse IP réseau du sous-réseau dans le champ **Adresse de début**. Entrez le masque de sous-réseau, tel que 255.255.255.0, dans le champ **Masque de sous-réseau**. Le champ affiche automatiquement une adresse de sous-réseau par défaut qui est basée sur l'adresse IP.

    IMPORTANT : évitez d'utiliser des sous-réseaux qui se chevauchent pour les sélecteurs de trafic distant et local. L'utilisation de ces sous-réseaux nécessite l'ajout de routes statiques sur le routeur et les hôtes à utiliser. Par exemple, évitez la combinaison suivante :

    Sélecteur de trafic local : 192.168.1.0/24

    Sélecteur de trafic distant : 192.168.0.0/16

Pour le type Stratégie **manuelle**, entrez les paramètres dans la section **Paramètres de stratégie manuelle**.

- **SPI-entrant, SPI-sortant** : saisissez une valeur hexadécimale composée de 3 à 8 caractères (0x1234, par exemple).
- **Algorithme de chiffrement** : sélectionnez l'algorithme utilisé pour chiffrer les données :
  - DES
  - 3DES
  - AES-128
  - AES-192
  - AES-256

- **Clé-entrante** : saisissez la clé de chiffrement de la stratégie appliquée au trafic entrant. La longueur de la clé dépend de l'algorithme de chiffrement choisi :
  - DES : 8 caractères
  - 3DES : 24 caractères
  - AES-128 : 16 caractères
  - AES-192 : 24 caractères
  - AES-256 : 32 caractères
- **Clé-sortante** : saisissez la clé de chiffrement de la stratégie appliquée au trafic sortant. La longueur de la clé dépend de l'algorithme de chiffrement choisi, comme indiqué ci-dessus.
- **Algorithme d'intégrité** : sélectionnez l'algorithme utilisé pour vérifier l'intégrité des données.
  - MD5
  - SHA-1
  - SHA2-256
- **Clé-entrante** : saisissez la clé d'intégrité (pour l'ESP avec mode d'intégrité) de la stratégie appliquée au trafic entrant. La longueur de la clé dépend de l'algorithme choisi :
  - MD5 : 16 caractères
  - SHA-1 : 20 caractères
  - SHA2-256 : 32 caractères
- **Clé-sortante** : saisissez la clé d'intégrité (pour l'ESP avec mode d'intégrité) de la stratégie appliquée au trafic sortant. La longueur de la clé dépend de l'algorithme choisi, comme indiqué ci-dessus.

Pour le type Stratégie **automatique**, entrez les paramètres dans la section **Paramètres de stratégie automatique**.

- **Durée de vie SA** : entrez la durée de l'association de sécurité en secondes. À la fin de l'intervalle indiqué en secondes, l'association de sécurité est renégociée. La valeur par défaut est 3 600 secondes. La valeur minimale est de 300 secondes.
- **Algorithme de chiffrement** : sélectionnez l'algorithme utilisé pour chiffrer les données.
- **Algorithme d'intégrité** : sélectionnez l'algorithme utilisé pour vérifier l'intégrité des données.
- **Groupe de clés PFS** : cochez la case **Activer** pour activer PFS (Perfect Forward Secrecy), afin de renforcer la sécurité. Ce protocole est plus lent, mais contribue à empêcher l'écoute électronique en garantissant qu'un échange Diffie-Hellman a lieu pour chaque négociation de phase 2.
- **Sélectionner la stratégie IKE** : sélectionnez la stratégie IKE qui définira les caractéristiques de la phase 1 de négociation. Cliquez sur **Afficher** pour afficher ou modifier la stratégie IKE existante qui est configurée sur le Cisco RV110W.

Configuration de la gestion des certificats

Le Cisco RV110W recourt à des certificats numériques pour l'authentification VPN IPsec et la validation SSL (pour HTTPS). Une fonctionnalité disponible sur le Cisco RV110W vous permet de générer et de signer vos propres certificats.

Génération d'un nouveau certificat

Vous pouvez générer un nouveau certificat en remplacement du certificat existant sur le Cisco RV110W.

Pour générer un certificat :

ÉTAPE 1 Sélectionnez **VPN** > **Gestion des certificats**.

ÉTAPE 2 Cliquez sur le bouton **Générer un nouveau certificat**.

ÉTAPE 3 Cliquez sur **Générer un certificat**.

Importation de certificats

Vous pouvez importer un certificat enregistré au préalable dans un fichier via le bouton **Exporter pour l'admin**.

Pour importer un certificat :

ÉTAPE 1 Sélectionnez **VPN** > **Gestion des certificats**.

ÉTAPE 2 Cliquez sur le bouton **Importer le certificat depuis un fichier**.

ÉTAPE 3 Cliquez sur **Parcourir** et recherchez le fichier de certificat.

ÉTAPE 4 Cliquez sur **Installer un certificat**.

Exportation de certificats pour l'administrateur

Le certificat pour l'administrateur contient la clé privée et doit être conservé en lieu sûr en guise de sauvegarde. Si la configuration du Cisco RV110W est rétablie sur ses paramètres d'usine, ce certificat peut ainsi être importé et restauré sur le routeur.

Pour exporter un certificat pour l'administrateur :

ÉTAPE 1 Sélectionnez **VPN** > **Gestion des certificats**.

ÉTAPE 2 Cliquez sur **Exporter pour l'admin**.

Sur un ordinateur, le gestionnaire de dispositifs enregistre le fichier admin.pem sous C:\Documents and Settings*ID_Utilisateur*\Mes documents\Téléchargements.

Exportation de certificats pour le client

Le certificat pour le client permet aux utilisateurs QuickVPN de se connecter en toute sécurité au Cisco RV110W. Les utilisateurs QuickVPN doivent placer le certificat dans le répertoire d'installation du client QuickVPN.

Pour exporter un certificat pour le client :

ÉTAPE 1 Sélectionnez **VPN** > **Gestion des certificats**.

ÉTAPE 2 Cliquez sur **Exporter pour le client**.

Sur un ordinateur, le Gestionnaire de périphérique enregistre le fichier client.pem sous C:\Documents and Settings*ID_Utilisateur*\Mes documents\Téléchargements.

Configuration de l'intercommunication VPN

L'intercommunication VPN permet au trafic VPN provenant des clients VPN de transiter par le Cisco RV110W.

Pour configurer l'intercommunication VPN :

ÉTAPE 1 Sélectionnez **VPN** > **Intercommunication VPN**.

ÉTAPE 2 Sélectionnez le type de trafic que le pare-feu autorise à transiter :

Intercommunication IPsec	Cochez **Activer** pour permettre aux tunnels de sécurité IP de transiter par le Cisco RV110W.
PPTP	Cochez **Activer** pour permettre aux tunnels PPTP de transiter par le Cisco RV110W.
L2TP	Cochez **Activer** pour permettre aux tunnels L2TP (Layer 2 Tunneling Protocol) de transiter par le Cisco RV110W.

ÉTAPE 3 Cliquez sur **Enregistrer**.

6

Configuration de la Qualité de service (QoS)

Le Cisco RV110W vous permet de configurer les fonctions QoS (Qualité de service) suivantes :

- **Configuration de la gestion de la bande passante, page 116**
- **Configuration des paramètres de port QoS, page 118**
- **Configuration des paramètres CoS, page 119**
- **Configuration des paramètres DSCP, page 120**

Configuration de la gestion de la bande passante

Vous pouvez utiliser la fonction de gestion de la bande passante du Cisco RV110W pour gérer la bande passante du trafic entre le réseau sécurisé (LAN) et le réseau non sécurisé (WAN).

Configuration de la bande passante

Configuration de la bande passante

Vous pouvez limiter la bande passante afin de réduire le débit de transmission de données du Cisco RV110W. Vous pouvez également utiliser un profil de bande passante pour limiter le trafic sortant, empêchant ainsi les utilisateurs du réseau LAN de consommer toute la bande passante de la liaison Internet.

Pour définir la bande passante montante et descendante :

ÉTAPE 1 Sélectionnez **QoS** > **Gestion de la bande passante**.

ÉTAPE 2 Dans le champ **Gestion de la bande passante**, cochez la case **Activer**. La bande passante maximale fournie par votre FAI s'affiche dans la section **Bande passante**.

ÉTAPE 3 Dans la **Table des bandes passantes**, saisissez les informations suivantes pour l'interface WAN :

Montant	La bande passante (kbit/s) utilisée pour envoyer des données sur Internet.
Descendant	La bande passante (kbit/s) utilisée pour recevoir des données d'Internet.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration des priorités de bande passante

Configuration des priorités de bande passante

Dans la **Table des priorités de bande passante**, vous pouvez affecter des priorités aux services pour gérer l'utilisation de la bande passante.

Pour configurer les priorités de bande passante :

ÉTAPE 1 Sélectionnez **QoS** > **Gestion de la bande passante**.

ÉTAPE 2 Dans le champ **Gestion de la bande passante**, cochez la case **Activer**. La bande passante maximale fournie par votre FAI s'affiche dans la section **Bande passante**.

ÉTAPE 3 Dans la **Table des priorités de bande passante**, cliquez sur **Ajouter une ligne**.

ÉTAPE 4 Saisissez les informations suivantes :

Activer	Cochez cette case pour activer la gestion de la bande passante pour ce service.
Service	Sélectionnez le service auquel attribuer la priorité.
Direction	Sélectionnez la direction du trafic que vous souhaitez privilégier (**Descendante** ou **Montante**).
Priorité	Sélectionnez le niveau de priorité du service (**Faible**, **Normal**, **Moyen** ou **Élevé**).

ÉTAPE 5 Cliquez sur **Enregistrer**.

Pour modifier les paramètres d'une entrée de la table, cochez la case correspondante, puis cliquez sur **Modifier**. Une fois les modifications terminées, cliquez sur **Enregistrer**.

Pour supprimer une entrée de la table, cochez la case correspondante, puis cliquez sur **Supprimer**. Cliquez ensuite sur **Enregistrer**.

Pour ajouter une nouvelle définition de service, cliquez sur le bouton **Gestion des services**. Vous pouvez définir un nouveau service à utiliser pour toutes les définitions de pare-feu et de QoS. Reportez-vous à la section **Configuration de la gestion de services**.

Configuration des paramètres de port QoS

Vous pouvez configurer les paramètres QoS pour chaque port LAN sur le Cisco RV110W. Le Cisco RV110W prend en charge 4 files d'attente de priorité pour la hiérarchisation du trafic par port commuté physique.

Pour configurer les paramètres QoS pour les ports LAN du Cisco RV110W :

ÉTAPE 1 Sélectionnez **QoS** > **Paramètres de port QoS**.

ÉTAPE 2 Pour chaque port de la **Table des paramètres de port QoS**, saisissez les informations suivantes :

Mode de confiance	Sélectionnez l'une des options suivantes dans le menu déroulant : ▪ **Port** : ce paramètre active le port d'après le QoS. Vous pouvez alors définir la priorité du trafic pour un port particulier. La priorité de la file d'attente de trafic commence avec le niveau de priorité le plus faible (1) et finit avec le niveau de priorité le plus élevé (4). ▪ **DSCP** : DSCP (Differentiated Services Code Point, point de code de services différenciés). L'activation de cette fonctionnalité privilégie le trafic réseau sur le LAN d'après le mappage de file d'attente DSCP sur la page **Paramètres DSCP**. ▪ **CoS** : CoS (Class of Service, classe de service).
File d'attente de transfert du trafic par défaut pour les appareils non validés	Sélectionnez un niveau de priorité pour le trafic sortant (de 1 à 4).

ÉTAPE 3 Cliquez sur **Enregistrer**.

Pour restaurer les paramètres de port QoS par défaut, cliquez sur **Restaurer les valeurs par défaut**. Cliquez ensuite sur **Enregistrer**.

Configuration des paramètres CoS

Vous pouvez mapper les paramètres de priorité CoS sur la file d'attente de transfert du trafic sur le Cisco RV110W.

Vous pouvez utiliser le lien vers la page Paramètres de port QoS pour mapper les paramètres de priorité CoS sur la file d'attente QoS.

Pour mettre en correspondance les paramètres de priorité CoS avec la file d'attente de transfert du trafic :

ÉTAPE 1 Sélectionnez **QoS** > **Paramètres CoS**.

ÉTAPE 2 Pour chaque niveau de priorité CoS dans la **Table des paramètres CoS**, sélectionnez une valeur de priorité dans le menu déroulant **File d'attente de transfert du trafic**.

Ces valeurs associent aux différents types de trafic des niveaux de priorité plus ou moins élevés.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Pour restaurer les paramètres de port QoS par défaut, cliquez sur **Restaurer les valeurs par défaut**. Cliquez ensuite sur **Enregistrer**.

Configuration des paramètres DSCP

Vous pouvez configurer le mappage DSCP à file d'attente QoS depuis la page **Paramètres DSCP**.

Pour configurer le mappage DSCP à file d'attente QoS :

ÉTAPE 1 Sélectionnez **QoS** > **Paramètres DSCP**.

ÉTAPE 2 Choisissez de répertorier uniquement les valeurs RFC ou toutes les valeurs DSCP dans la **Table des paramètres DSCP** en cliquant sur le bouton correspondant.

ÉTAPE 3 Pour chaque valeur DSCP dans la **Table des paramètres DSCP**, sélectionnez un niveau de priorité dans le menu déroulant **File d'attente**.

Cela associe la valeur DSCP avec la file d'attente QoS sélectionnée.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Pour restaurer les paramètres DSCP par défaut, cliquez sur **Restaurer les valeurs par défaut**. Cliquez ensuite sur **Enregistrer**.

7

Administration de votre Cisco RV110W

Ce chapitre décrit les fonctions d'administration du Cisco RV110W, notamment la création d'utilisateurs, la gestion réseau, le diagnostic système et la journalisation, la date et l'heure, ainsi que d'autres paramètres.

- Définition de la complexité des mots de passe, page 122
- Configuration des comptes d'utilisateurs, page 123
- Définition du délai d'expiration de session, page 124
- Configuration SNMP (Simple Network Management Protocol), page 124
- Utilisation des outils de diagnostic, page 127
- Configuration de la journalisation, page 130
- Configuration de Bonjour, page 134
- Configuration des paramètres de date et d'heure, page 135
- Sauvegarde et restauration du système, page 136
- Mise à niveau du micrologiciel ou modification de la langue, page 139
- Redémarrage du Cisco RV110W, page 141
- Restauration des paramètres d'usine, page 141

Définition de la complexité des mots de passe

Le Cisco RV110W peut exiger une complexité minimale du mot de passe lors des changements de mot de passe.

Pour configurer les paramètres de complexité du mot de passe :

ÉTAPE 1 Sélectionnez **Administration** > **Complexité du mot de passe**.

ÉTAPE 2 Dans le champ **Paramètres de complexité du mot de passe**, cochez la case **Activer**.

ÉTAPE 3 Configurez les paramètres de complexité du mot de passe :

Longueur minimale du mot de passe	Saisissez la longueur minimale du mot de passe (entre 0 et 64 caractères).
Nombre minimal de classes de caractères	Saisissez un nombre correspondant à l'une des classes de caractères suivantes : ▪ Lettres majuscules ▪ Lettres minuscules ▪ Chiffres ▪ Caractères spéciaux disponibles sur un clavier standard Par défaut, les mots de passe doivent contenir des caractères d'au moins trois de ces classes.
Le nouveau mot de passe doit être différent de l'actuel	Cochez la case **Activer** pour exiger que les nouveaux mots de passe soient différents du mot de passe actuel.
Expiration du mot de passe	Cochez la case **Activer** pour que les mots de passe expirent après un délai donné.
Délai d'expiration du mot de passe	Saisissez le nombre de jours au bout duquel le mot de passe expire (1–365). La valeur par défaut est de 180 jours.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration des comptes d'utilisateurs

Le Cisco RV110W prend en charge deux comptes d'utilisateurs pour l'administration et l'affichage des paramètres : un administrateur (nom d'utilisateur et mot de passe par défaut : « cisco ») et un invité (nom d'utilisateur par défaut : « guest »).

Le compte invité (guest) est en lecture seule. Vous pouvez définir et modifier le nom d'utilisateur et le mot de passe des comptes administrateur et invité.

Pour configurer les comptes d'utilisateurs :

ÉTAPE 1 Sélectionnez **Administration** > **Utilisateurs**.

ÉTAPE 2 Dans le champ **Activation du compte**, cochez les cases des comptes que vous souhaitez activer. (Le compte administrateur doit être actif.)

ÉTAPE 3 (Optional) Pour modifier le compte administrateur, sous **Paramètre du compte administrateur**, cochez **Modifier les paramètres administrateur**. Pour modifier le compte invité, sous **Paramètres d'invité**, cochez **Modifier les paramètres d'invité**. Saisissez les informations suivantes :

Nouveau nom d'utilisateur	Saisissez un nouveau nom d'utilisateur.
Ancien mot de passe	Saisissez le mot de passe actuel.
Nouveau mot de passe	Saisissez le nouveau mot de passe. Veillez à ce que le mot de passe ne contienne aucun mot du dictionnaire quelle que soit la langue et à ce qu'il contienne des lettres (majuscules et minuscules), des chiffres et des symboles. Le mot de passe peut comporter au maximum 64 caractères.
Confirmer le nouveau mot de passe	Ressaisissez le nouveau mot de passe.

ÉTAPE 4 Pour importer des noms d'utilisateurs et des mots de passe d'un fichier CSV :

a. Dans le champ **Importer le nom de l'utilisateur et le mot de passe**, cliquez sur **Parcourir**.

b. Trouvez le fichier et cliquez sur **Ouvrir**.

c. Cliquez sur **Importer**.

ÉTAPE 5 Saisissez l'ancien mot de passe.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Définition du délai d'expiration de session

Le délai d'expiration est le nombre de minutes d'inactivité autorisé avant la fermeture de la session du gestionnaire de dispositifs. Vous pouvez configurer le délai d'expiration pour les comptes administrateur et invité.

Pour configurer le délai d'expiration de la session :

ÉTAPE 1 Sélectionnez **Administration** > **Délai d'expiration de session**.

ÉTAPE 2 Dans le champ **Délai d'expiration d'inactivité d'administrateur**, saisissez le nombre de minutes avant l'expiration d'une session pour cause d'inactivité. Choisissez **jamais** pour permettre à l'administrateur de rester connecté en permanence.

ÉTAPE 3 Dans le champ **Délai d'expiration d'inactivité d'invité**, saisissez le nombre de minutes avant l'expiration d'une session pour cause d'inactivité. Choisissez **jamais** pour permettre à l'administrateur de rester connecté en permanence.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration SNMP (Simple Network Management Protocol)

Le protocole SNMP (Simple Network Management Protocol) vous permet de surveiller et de gérer le routeur depuis un gestionnaire SNMP. Le protocole SNMP est une solution de surveillance et de contrôle des appareils réseau à distance, qui permet également la gestion des configurations, la collecte de statistiques, des performances et de la sécurité.

Configuration des informations système SNMP

Configuration des informations système SNMP

Dans la section **Informations système SNMP** de la page **SNMP**, vous pouvez activer SNMP.

Avant de pouvoir utiliser SNMP, vous devez installer le logiciel SNMP sur l'ordinateur. Le Cisco RV110W prend uniquement en charge SNMPv3 pour la gestion SNMP. Le Cisco RV110W prend en charge SNNPv1/2/3 pour les messages « trap » SNMP.

Pour activer SNMP :

ÉTAPE 1 Sélectionnez **Administration** > **SNMP**.

ÉTAPE 2 Cochez la case **Activer** pour activer l'option SNMP.

ÉTAPE 3 Saisissez les informations suivantes :

SysContact	Saisissez le nom de la personne à contacter pour ce pare-feu (par exemple, **admin** ou **Jean Durand**).
SysLocation	Saisissez l'emplacement physique du pare-feu (par exemple, **Rack n° 2, 4e étage**).
SysName	Saisissez un nom pour une identification facile du pare-feu.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Modification des utilisateurs SNMPv3

Modification des utilisateurs SNMPv3

Vous pouvez configurer les paramètres SNMPv3 pour les deux comptes d'utilisateurs par défaut du Cisco RV110W (admin et invité).

Pour configurer les paramètres SNMPv3 :

ÉTAPE 1 Sélectionnez **Administration** > **SNMP**.

ÉTAPE 2 Sous **Configuration utilisateur SNMPv3**, configurez les paramètres suivants :

Nom d'utilisateur	Sélectionnez le compte à configurer (**admin** ou **invité**).
Autorisation d'accès	Affiche les privilèges d'accès du compte d'utilisateur sélectionné.
Niveau de sécurité	Choisissez le niveau de sécurité SNMPv3 : **Aucune authentification et aucun privilège** : ne nécessite ni authentification ni confidentialité. **Authentification et aucun privilège** : soumettez uniquement l'algorithme d'authentification et le mot de passe. **Authentification et privilège** : soumettez l'algorithme d'authentification/confidentialité et le mot de passe.
Serveur d'algorithmes d'authentification	Sélectionnez le type d'algorithme d'authentification (**MD5** ou **SHA**).
Mot de passe d'authentification	Saisissez le mot de passe d'authentification.
Algorithme de confidentialité	Sélectionnez le type d'algorithme de confidentialité (**DES** ou **AES**)
Mot de passe de confidentialité	Saisissez le mot de passe de confidentialité.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration des filtres SNMP

Configuration des filtres SNMP

Les champs de la section **Configuration de filtre** de **SNMP** vous permettent de configurer un agent SNMP auquel le pare-feu envoie les messages d'interception (notifications).

Pour configurer les filtres :

ÉTAPE 1 Sélectionnez **Administration** > **SNMP**.

ÉTAPE 2 Sous **Configuration de filtre**, configurez les paramètres suivants :

Adresse IP	Saisissez l'adresse IP du gestionnaire SNMP ou de l'agent de filtre.
Port	Saisissez le port du filtre SNMP de l'adresse IP à laquelle les messages « trap » seront envoyés.
Communauté	Saisissez la chaîne de communauté à laquelle appartient l'agent. La plupart des agents sont configurés pour écouter les filtres dans la communauté publique.
Version SNMP	Sélectionnez la version SNMP : **v1**, **v2c** ou **v3**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Utilisation des outils de diagnostic

Le Cisco RV110W fournit plusieurs outils de diagnostic qui vous aident dans la résolution des problèmes réseau.

- **Outils réseau**
- **Configuration de la mise en miroir des ports**

Outils réseau

Utilisez les outils réseau pour résoudre les problèmes réseau.

Utilisation de l'outil PING

Vous pouvez utiliser l'utilitaire PING pour tester la connectivité entre ce routeur et un autre périphérique du réseau. Vous pouvez également utiliser l'outil PING pour tester la connectivité à Internet en envoyant une requête Ping à un nom de domaine complet (par exemple, www.cisco.com).

Pour utiliser l'outil PING :

ÉTAPE 1 Sélectionnez **Administration** > **Diagnostic** > **Outils réseau**.

ÉTAPE 2 Dans le champ **Adresse IP/nom de domaine**, saisissez l'adresse IP du périphérique ou un nom de domaine complet, tel que www.cisco.com, où envoyer la requête Ping.

ÉTAPE 3 Cliquez sur **Ping**. Les résultats de la requête Ping s'affichent. Ces résultats indiquent si le périphérique est joignable.

ÉTAPE 4 Cliquez sur **Fermer** lorsque vous avez terminé.

Utilisation de Traceroute

L'utilitaire Traceroute affiche tous les routeurs présents entre l'adresse IP de destination et ce routeur. Le routeur affiche jusqu'à 30 sauts (routeurs intermédiaires) entre ce routeur et la destination.

Pour utiliser Traceroute :

ÉTAPE 1 Sélectionnez **Administration** > **Diagnostic** > **Outils réseau**.

ÉTAPE 2 Dans le champ **Adresse IP/nom de domaine**, saisissez l'adresse IP à suivre.

ÉTAPE 3 Cliquez sur **Traceroute**. Les résultats Traceroute s'affichent.

ÉTAPE 4 Cliquez sur **Fermer** lorsque vous avez terminé.

Recherche DNS

Vous pouvez utiliser l'outil de recherche pour trouver l'adresse IP d'un hôte (par exemple, un serveur Web, FTP ou de messagerie) sur Internet.

Pour récupérer l'adresse IP d'un serveur Web, FTP, de messagerie ou autre sur Internet, saisissez le Nom Internet dans la zone de texte correspondante, puis cliquez sur **Rechercher**. Si l'hôte ou le domaine saisi existe, vous obtenez une réponse contenant l'adresse IP. Le message « Hôte inconnu » indique que le nom Internet spécifié n'existe pas.

Pour utiliser l'outil de recherche :

ÉTAPE 1 Sélectionnez **Administration** > **Diagnostic** > **Outils réseau**.

ÉTAPE 2 Dans le champ **Nom Internet**, saisissez le nom Internet de l'hôte.

ÉTAPE 3 Cliquez sur **Rechercher**. Les résultats de la recherche s'affichent.

ÉTAPE 4 Cliquez sur **Fermer** lorsque vous avez terminé.

Configuration de la mise en miroir des ports

La mise en miroir des ports surveille le trafic réseau en envoyant des copies de tous les paquets entrants et sortants d'un port à un port de surveillance. La mise en miroir des ports peut servir d'outil de diagnostic ou de débogage, en particulier pour repousser une attaque ou pour surveiller le trafic utilisateur de LAN à WAN afin de voir si les utilisateurs accèdent à des informations ou à des sites Web inappropriés.

L'hôte LAN (PC) doit utiliser une adresse IP statique pour éviter tout problème avec la mise en miroir des ports. Les baux DHCP d'un hôte LAN peuvent expirer et entraîner l'échec de la mise en miroir des ports si une adresse IP statique n'est pas configurée pour l'hôte LAN.

Pour configurer la mise en miroir des ports :

ÉTAPE 1 Sélectionnez **Administration** > **Diagnostic** > **Mise en miroir de ports**.

ÉTAPE 2 Dans le champ **Source miroir**, sélectionnez les ports à mettre en miroir.

ÉTAPE 3 Dans le menu déroulant **Mettre le port en miroir**, sélectionnez un port miroir. Si vous utilisez un port pour la mise en miroir, ne l'utilisez pas pour d'autres types de trafic.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration de la journalisation

Le Cisco RV110W vous permet de configurer les options de journalisation.

Configuration des paramètres de journalisation

Pour configurer la journalisation :

ÉTAPE 1 Sélectionnez **Administration** > **Journalisation** > **Paramètres des journaux**.

ÉTAPE 2 Dans le champ **Mode journalisation**, cochez la case **Activer**.

ÉTAPE 3 Cliquez sur **Ajouter une ligne**.

ÉTAPE 4 Configurez les paramètres suivants :

Serveur de journalisation distant	Saisissez l'adresse IP du serveur de journalisation qui recueille les journaux.
Indiquer la gravité pour le journal local et e-mail	Cliquez pour choisir la sévérité des journaux que vous souhaitez configurer. Notez que tous les types de journaux au-delà d'un type sélectionné sont automatiquement inclus et qu'il n'est pas possible de les désélectionner. Par exemple, choisir des journaux « erreur » entraîne la sélection des journaux critiques, d'urgence et d'alerte, en plus des journaux d'erreur. Les niveaux de sévérité des événements sont répertoriés du niveau le plus élevé au plus faible, comme suit : ▪ **Urgence** : le système n'est pas utilisable. ▪ **Alerte** : une action est requise. ▪ **Critique** : le système est dans un état critique. ▪ **Erreur** : le système subit une condition d'erreur. ▪ **Avertissement** : un avertissement système a été généré. ▪ **Notification** : le système fonctionne correctement, mais une notification système a été générée. ▪ **Information** : informations du périphérique. ▪ **Débogage** : fournit des informations détaillées sur un événement. La sélection de cette option de sévérité entraîne la génération de grandes quantités de journaux et n'est pas recommandée dans le cadre d'un fonctionnement normal du routeur.
Activer	Cochez cette case pour activer ces paramètres de journalisation.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Pour modifier une entrée dans la **Table des paramètres de journalisation**, sélectionnez l'entrée en question, puis cliquez sur **Modifier**. Apportez les modifications voulues, puis cliquez sur **Enregistrer**.

Configuration de l'envoi des journaux par e-mail

Vous pouvez configurer le Cisco RV110W afin qu'il envoie les journaux par e-mail. Nous vous recommandons de configurer un compte de messagerie distinct pour l'envoi et la réception des journaux.

Vous devez commencer par configurer la sévérité des journaux à capturer ; voir la section **Configuration des paramètres de journalisation**.

Pour configurer l'envoi des journaux par e-mail :

ÉTAPE 1 Sélectionnez **Administration** > **Journalisation** > **Paramètres d'e-mail**.

ÉTAPE 2 Cochez la case **Activer** pour activer l'envoi des événements de journalisation par e-mail.

ÉTAPE 3 La sévérité minimale des journaux à capturer s'affiche. Pour la modifier, cliquez sur **Configurer la sévérité**.

ÉTAPE 4 Configurez les paramètres suivants :

Adresse du serveur de messagerie	Saisissez l'adresse IP du serveur SMTP. Il s'agit du serveur de messagerie associé au compte de messagerie que vous avez configuré (*mail.nom_entreprise.com*, par exemple).
Port du serveur de messagerie	Saisissez le port du serveur SMTP. Si votre fournisseur de messagerie demande un port spécial pour le courrier électronique, entrez-le à cet emplacement. Dans le cas contraire, utilisez la valeur par défaut (25).

Adresse e-mail de l'expéditeur	Entrez l'adresse e-mail de retour à laquelle le Cisco RV110W enverra les messages si les journaux provenant du serveur et acheminés à l'adresse e-mail de destination ne peuvent pas être distribués.
Adresse e-mail de destination (1)	Saisissez une adresse e-mail à laquelle envoyer les journaux (*logging@nom_entreprise.com*, par exemple).
Adresse e-mail de destination (2) (facultatif)	Saisissez une adresse e-mail supplémentaire à laquelle envoyer les journaux.
Adresse e-mail de destination (3) (facultatif)	Saisissez une adresse e-mail supplémentaire à laquelle envoyer les journaux.
Chiffrement e-mail (SSL)	Cochez la case **Activer** pour activer le chiffrement e-mail.
Authentification avec serveur SMTP	Si le serveur (de messagerie) SMTP exige une authentification avant d'accepter les connexions, sélectionnez le type d'authentification dans le menu déroulant : **Aucun**, **CONNEXION**, **SIMPLE** et **CRAM-MD5**.
Nom d'utilisateur d'authentification e-mail	Entrez le nom d'utilisateur d'authentification e-mail (*logging@nom_entreprise.com*, par exemple).
Mot de passe d'authentification e-mail	Entrez le mot de passe d'authentification e-mail (par exemple, le mot de passe utilisé pour accéder au compte de messagerie que vous avez configuré pour l'envoi des journaux).
Test d'authentification e-mail	Cliquez sur **Test** pour tester l'authentification e-mail.

ÉTAPE 5 Dans la section **Envoyer les journaux par e-mail selon un horaire**, configurez les paramètres suivants :

Unité	Sélectionnez l'unité de temps pour les journaux (**Jamais**, **Toutes les heures**, **Tous les jours** ou **Toutes les semaines**). Si vous sélectionnez **Jamais**, les journaux ne sont pas envoyés.
Jour	Si vous choisissez un horaire hebdomadaire pour envoyer les journaux, sélectionnez le jour de la semaine auquel envoyer les journaux.
Heure	Si vous choisissez un horaire quotidien ou hebdomadaire pour envoyer les journaux, sélectionnez l'heure de la journée à laquelle envoyer les journaux.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Configuration de Bonjour

Bonjour est un protocole de découverte et d'annonce de service. Sur le Cisco RV110W, Bonjour doit être activé pour annoncer les services par défaut configurés sur le périphérique.

Pour activer Bonjour :

ÉTAPE 1 Sélectionnez **Administration** > **Bonjour**.

ÉTAPE 2 Cochez la case **Activer** pour activer le protocole Bonjour.

ÉTAPE 3 Pour activer Bonjour pour un réseau VLAN répertorié dans la **Table de contrôle des interfaces Bonjour**, cochez la case **Activer Bonjour** correspondante.

Vous pouvez activer Bonjour sur des réseaux VLAN spécifiques. L'activation de Bonjour sur un réseau VLAN permet aux périphériques présents sur le réseau VLAN de découvrir les services Bonjour disponibles sur le routeur (tels que http/https).

Par exemple, si un réseau VLAN est configuré avec un ID de 2, les périphériques et les hôtes présents sur un réseau VLAN 2 ne peuvent pas découvrir les services Bonjour exécutés sur le routeur à moins que Bonjour soit activé pour VLAN 2.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration des paramètres de date et d'heure

Vous pouvez configurer votre fuseau horaire, indiquer s'il faut ou non prendre en compte l'heure d'été et définir le serveur NTP (Network Time Protocol) avec lequel synchroniser la date et l'heure. Le routeur obtient alors ses informations de date et d'heure du serveur NTP.

Pour configurer les paramètres NTP et d'heure :

ÉTAPE 1 Sélectionnez **Administration** > **Paramètres de l'heure**. L'heure actuelle s'affiche.

ÉTAPE 2 Précisez les informations suivantes :

Fuseau horaire	Sélectionnez votre fuseau horaire par rapport à l'heure de Greenwich (GMT).
Prendre en compte l'heure d'été	Si cela est pertinent pour votre zone géographique, cochez la case **Prendre en compte l'heure d'été**. Cette option est disponible lorsque vous cliquez sur **Automatique** dans le champ **Définir la date et l'heure** plus bas.
Mode heure d'été	Choisissez **Par date** (vous devez alors indiquer la date à laquelle le mode heure d'été commence) ou **Récurrent** (vous devez alors indiquer le mois, la semaine, le jour de la semaine et l'heure à laquelle l'heure d'été commence). Fournissez les informations dans les champs « de » et « à ».
Décalage dû à l'heure d'été	Dans le menu déroulant, sélectionnez le décalage par rapport au temps universel coordonné (UTC).

Définir la date et l'heure	Sélectionnez le mode de définition de la date et de l'heure.
Serveur NTP	Pour utiliser les serveurs NTP par défaut, cliquez sur le bouton **Valeurs par défaut**. Pour utiliser un serveur NTP spécifique, cliquez sur **Serveur NTP défini par l'utilisateur** et saisissez le nom de domaine complet ou l'adresse IP du serveur NTP dans les deux champs disponibles.
Saisir la date et l'heure	Saisissez la date et l'heure.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Sauvegarde et restauration du système

Vous pouvez sauvegarder les paramètres de configuration personnalisés pour une restauration ultérieure ou restaurer depuis une précédente sauvegarde à partir de la page **Administration** > **Paramètres de sauvegarde/restauration**.

Lorsque le pare-feu fonctionne tel que configuré, vous pouvez sauvegarder la configuration pour une restauration ultérieure. Lors de la sauvegarde, vos paramètres sont enregistrés sous la forme d'un fichier sur votre ordinateur. Vous pouvez restaurer les paramètres du pare-feu à partir de ce fichier.

ATTENTION Lors d'une restauration, n'essayez pas de naviguer en ligne, ne désactivez pas le pare-feu, n'arrêtez pas l'ordinateur et n'utilisez pas le pare-feu jusqu'au terme de l'opération. Celle-ci devrait prendre environ une minute. Lorsque le voyant de test s'éteint, patientez encore quelques secondes avant d'utiliser le pare-feu.

Sauvegarde des paramètres de configuration

Sauvegarde des paramètres de configuration

Pour sauvegarder ou restaurer la configuration :

ÉTAPE 1 Sélectionnez **Administration** > **Paramètres de sauvegarde/restauration**.

ÉTAPE 2 Sélectionnez la configuration à sauvegarder ou à effacer :

Configuration de démarrage	Sélectionnez cette option pour télécharger la configuration de démarrage. La configuration de démarrage est la configuration d'exécution la plus couramment utilisée par le Cisco RV110W. En cas de perte de la configuration de démarrage du routeur, utilisez cette page pour copier la configuration de secours vers la configuration de démarrage et restaurer les informations de configuration antérieures. Vous pouvez télécharger la configuration de démarrage vers d'autres Cisco RV110W pour un déploiement facile.
Configuration miroir	Sélectionnez cette option pour commander au Cisco RV110W de sauvegarder la configuration de démarrage après 24 heures de fonctionnement sans aucune modification dans la configuration de démarrage.
Configuration de secours	Sélectionnez cette option pour sauvegarder les paramètres de configuration actuels.

ÉTAPE 3 Pour télécharger un fichier de sauvegarde d'après l'option de configuration sélectionnée, cliquez sur **Télécharger**.

Par défaut, le fichier (startup.cfg, mirror.cfg ou backup.cfg) est téléchargé dans le dossier Téléchargements par défaut ; par exemple, *C:\Documents and Settings\admin\Mes documents\Téléchargements*.

ÉTAPE 4 Pour effacer la configuration sélectionnée, cliquez sur **Effacer**.

Restauration des paramètres de configuration

Restauration des paramètres de configuration

Vous pouvez restaurer un fichier de configuration préalablement enregistré :

ÉTAPE 1 Sélectionnez **Administration** > **Paramètres de sauvegarde/restauration**.

ÉTAPE 2 Dans le champ Téléchargement de la configuration, sélectionnez la configuration à charger (**Configuration de démarrage** ou **Configuration de secours**).

ÉTAPE 3 Cliquez sur **Parcourir** pour trouver le fichier.

ÉTAPE 4 Sélectionnez le fichier, puis cliquez sur **Ouvrir**.

ÉTAPE 5 Cliquez sur **Lancer le téléchargement**.

Le Cisco RV110W charge le fichier de configuration et utilise les paramètres qu'il contient pour mettre à jour la configuration de démarrage. Ensuite, le Cisco RV110W redémarre et utilise la nouvelle configuration.

Copie des paramètres de configuration

Copie des paramètres de configuration

Vous pouvez copier la configuration de démarrage dans la configuration de secours pour être sûr de disposer d'une copie de secours si vous oubliez votre nom d'utilisateur et votre mot de passe et que vous ne parvenez plus à accéder au gestionnaire de dispositifs. Dans ce cas, le seul moyen d'accéder au gestionnaire de dispositifs est de rétablir les paramètres par défaut du Cisco RV110W.

Le fichier de configuration de secours reste en mémoire et permet de copier les informations de configuration sauvegardées vers la configuration de démarrage, qui restaure l'ensemble des paramètres.

Pour copier une configuration (par exemple, pour copier une configuration de démarrage vers la configuration de secours) :

ÉTAPE 1 Sélectionnez **Administration** > **Paramètres de sauvegarde/restauration**.

ÉTAPE 2 Dans le champ **Copier**, sélectionnez les configurations source et destination dans les menus déroulants.

ÉTAPE 3 Cliquez sur **Lancer la copie**.

Génération d'une clé de chiffrement

Génération d'une clé de chiffrement

Le routeur vous permet de générer une clé de chiffrement pour protéger les fichiers de secours.

Pour générer une clé de chiffrement :

ÉTAPE 1 Sélectionnez **Administration** > **Paramètres de sauvegarde/restauration**.

ÉTAPE 2 Cliquez sur **Afficher les paramètres avancés**.

ÉTAPE 3 Dans la case, saisissez la valeur de départ utilisée pour générer la clé.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Mise à niveau du micrologiciel ou modification de la langue

Vous pouvez mettre à niveau le micrologiciel vers une version plus récente ou modifier la langue du routeur depuis la page **Administration** > **Mise à niveau du micrologiciel/de la langue**.

ATTENTION Lors d'une mise à niveau du micrologiciel, n'essayez pas de naviguer en ligne, ne désactivez pas l'appareil, n'arrêtez pas l'ordinateur et n'interrompez surtout pas le processus jusqu'au terme de l'opération. Ce processus prend environ une minute, redémarrage inclus. L'interruption du processus de mise à niveau à certains moments de l'écriture de la mémoire flash peut la corrompre et rendre le routeur inutilisable.

Mise à niveau du micrologiciel

Pour mettre à niveau le micrologiciel vers une version plus récente :

ÉTAPE 1 Sélectionnez **Administration** > **Mise à niveau du micrologiciel/de la langue**.

ÉTAPE 2 (Facultatif) Cliquez sur **Télécharger** pour télécharger la dernière version du micrologiciel.

ÉTAPE 3 Dans le champ **Type de fichier**, cliquez sur le bouton **Image du micrologiciel**.

ÉTAPE 4 Cliquez sur **Parcourir** pour trouver et sélectionner le micrologiciel téléchargé.

ÉTAPE 5 (Facultatif) Pour restaurer les paramètres par défaut du Cisco RV110W après une mise à niveau du micrologiciel, cochez la case **Rétablir tous les paramètres/configurations d'usine**.

ATTENTION La restauration des paramètres par défaut du Cisco RV110W efface tous vos paramètres personnalisés.

ÉTAPE 6 Cliquez sur **Démarrer la mise à niveau**.

Une fois validée, la nouvelle image du micrologiciel est enregistrée dans la mémoire flash et le routeur est automatiquement redémarré avec le nouveau micrologiciel.

ÉTAPE 7 Sélectionnez **État** > **Récapitulatif du système** pour vous assurer que le routeur a installé la nouvelle version du micrologiciel.

Modification de la langue

Pour modifier la langue :

ÉTAPE 1 Sélectionnez **Administration** > **Mise à niveau du micrologiciel/de la langue**.

ÉTAPE 2 Dans le champ **Type de fichier**, cliquez sur le bouton **Fichier de langue**.

ÉTAPE 3 Cliquez sur **Parcourir** pour localiser et sélectionner le fichier de langue.

ÉTAPE 4 Cliquez sur **Démarrer la mise à niveau**.

Redémarrage du Cisco RV110W

Pour redémarrer le routeur :

ÉTAPE 1 Sélectionnez **Administration** > **Redémarrer**.

ÉTAPE 2 Cliquez sur **Redémarrer**.

Restauration des paramètres d'usine

ATTENTION Lors d'une restauration, n'essayez pas de naviguer en ligne, ne désactivez pas le routeur, n'arrêtez pas l'ordinateur et n'utilisez pas le routeur jusqu'au terme de l'opération. Celle-ci devrait prendre environ une minute. Lorsque le voyant de test s'éteint, patientez encore quelques secondes avant d'utiliser le routeur.

Pour rétablir les paramètres d'usine du routeur :

ÉTAPE 1 Sélectionnez **Administration** > **Rétablir les paramètres d'usine**.

ÉTAPE 2 Cliquez sur **Par défaut**.

Exécution de l'assistant de configuration

Pour exécuter l'assistant de configuration :

ÉTAPE 1 Sélectionnez **Administration** > **Assistant de configuration**.

ÉTAPE 2 Suivez les instructions en ligne.

8

Affichage de l'état du Cisco RV110W

Ce chapitre indique comment consulter des statistiques en temps réel et d'autres informations sur le Cisco RV110W.

- **Affichage du tableau de bord, page 143**
- **Affichage du récapitulatif du système, page 145**
- **Affichage des statistiques relatives au réseau sans fil, page 148**
- **Affichage de l'état du VPN, page 149**
- **Affichage des journaux, page 151**
- **Affichage des périphériques connectés, page 152**
- **Affichage des statistiques des ports, page 153**

Affichage du tableau de bord

La page **Tableau de bord** offre une vue d'ensemble sur les informations importantes concernant le routeur.

Pour afficher le tableau de bord :

ÉTAPE 1 Sélectionnez **État** > **Tableau de bord**.

ÉTAPE 2 Pour afficher une vue interactive du panneau arrière du routeur, cliquez sur **Afficher le panneau arrière du routeur**.

L'affichage du panneau arrière indique les ports utilisés (en vert) et vous permet de cliquer sur chaque port pour obtenir des informations relatives à la connexion.

- Pour afficher les informations de connexion d'un port, cliquez sur celui-ci.
- Pour actualiser les informations sur le port, cliquez sur **Actualiser**.
- Pour fermer la fiche d'information sur le port, cliquez sur **Fermer**.

La page **Tableau de bord** affiche les éléments suivants :

Informations concernant l'appareil

- **Nom du système** : nom de l'appareil.
- **Version du micrologiciel** : version actuelle du logiciel exécuté par l'appareil.
- **Numéro de série** : numéro de série de l'appareil.

Utilisation des ressources

- **UC** : utilisation du processeur.
- **Mémoire** : utilisation de la mémoire.
- **Heure actuelle** : heure du jour.
- **Durée de disponibilité système** : durée de fonctionnement du système.

Récapitulatif Syslog

Indique si la journalisation est activée pour ces catégories d'événement :

- **Urgence**
- **Alerte**
- **Critique**
- **Erreurs**
- **Avertissement**

Pour afficher les journaux, cliquez sur **détails**. Pour plus d'informations, reportez-vous à la section **Affichage des journaux**.

Pour gérer les journaux, cliquez sur **gérer la journalisation**. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres de journalisation**.

Interface LAN (réseau local)

- **Adresse MAC** : adresse MAC du routeur.
- **Adresse IPv4** : adresse IP locale du routeur.
- **Adresse IPv6** : adresse IP locale du routeur (si IPv6 est activé).
- **Serveur DHCP** : état du serveur DHCP IPv4 du routeur (activé ou désactivé).
- **Serveur DHCPv6** : état du serveur DHCP IPv6 du routeur (activé ou désactivé).

Pour afficher les paramètres LAN, cliquez sur **détails**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des paramètres LAN**.

Informations WAN (Internet)

- **Adresse IPv4** : adresse IP du port WAN du routeur.
- **Adresse IPv6** : adresse IP du port WAN du routeur, si IPv6 est activé.
- **État** : état de la connexion Internet (montante ou descendante).

Pour afficher les paramètres WAN, cliquez sur **détails**. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres WAN**.

Réseaux sans fil

Répertorie l'état des quatre SSID de réseau sans fil.

Pour afficher les paramètres sans fil du routeur, cliquez sur **détails**. Pour plus d'informations, reportez-vous à la section **Affichage des statistiques relatives au réseau sans fil**.

VPN

- **Utilisateurs QuickVPN** : nombre d'utilisateurs QuickVPN.
- **Utilisateurs PPTP** : nombre d'utilisateurs PPTP (Point-to-Point Tunneling Protocol).

Affichage du récapitulatif du système

La page **Récapitulatif du système** affiche un récapitulatif des paramètres du routeur.

Pour afficher un récapitulatif des paramètres système :

ÉTAPE 1 Sélectionnez **État** > **Récapitulatif du système**.

ÉTAPE 2 Cliquez sur **Actualiser** pour obtenir les informations les plus récentes.

La page **Récapitulatif du système** affiche les informations suivantes :

Informations système

- **Version du micrologiciel** : version actuelle du logiciel exécuté par l'appareil.
- **Somme de contrôle MD5 du micrologiciel** : algorithme Message-Digest utilisé pour vérifier l'intégrité des fichiers.
- **Paramètres régionaux** : langue installée sur le routeur.
- **Version de langue** : version du module linguistique installé. La version du module linguistique doit être compatible avec le micrologiciel actuellement installé. Dans certains cas, un module linguistique plus ancien peut être utilisé avec une image plus récente du micrologiciel. Le routeur vérifie la version du module linguistique pour voir si elle est compatible avec la version actuelle du micrologiciel.

- **Somme de contrôle MD5 de langue** : somme de contrôle MD5 du module linguistique.
- **Modèle d'UC** : jeu de puces (chipset) du processeur actuellement utilisé.
- **Numéro de série** : numéro de série de l'appareil.
- **Durée de disponibilité système** : durée de fonctionnement du système.
- **Heure actuelle** : heure du jour.
- **PID VID** : ID de produit et ID de version de l'appareil.

Configuration IPv4

- **IP du réseau LAN** : adresse LAN du périphérique.
- **IP WAN** : adresse WAN du périphérique. Vous pouvez libérer l'adresse IP actuelle et en obtenir une nouvelle en cliquant sur **Libérer** ou sur **Renouveler**.
- **Passerelle** : adresse IP de la passerelle à laquelle le Cisco RV110W est connecté (le modem câble, par exemple).
- **Mode** : affiche **Passerelle** si la fonctionnalité NAT est activée, sinon **Routeur**.
- **DNS 1** : adresse IP du serveur DNS principal du port WAN.
- **DNS 2** : adresse IP du serveur DNS secondaire du port WAN.
- **DDNS** : indique si DNS dynamique est activé ou désactivé.

Configuration IPv6

- **IP du réseau LAN** : adresse LAN du périphérique.
- **IP WAN** : adresse WAN du périphérique.
- **Passerelle** : adresse IP de la passerelle à laquelle le Cisco RV110W est connecté (le modem câble, par exemple).
- **NTP** : serveur NTP (Network Time Protocol) (nom d'hôte ou adresse IPv6).
- **Délégation du préfixe** : préfixe IPv6 transmis du périphérique au FAI et qui est attribué aux adresses IP sur le Cisco RV110W.
- **DNS 1** : adresse IP du serveur DNS principal.
- **DNS 2** : adresse IP du serveur DNS secondaire.

Récapitulatif sans fil

- **SSID 1** : nom public du premier réseau sans fil.
  - **Sécurité** : paramètre de sécurité pour SSID 1.
- **SSID 2** : nom public du second réseau sans fil.
  - **Sécurité** : paramètre de sécurité pour SSID 2.
- **SSID 3** : nom public du troisième réseau sans fil.
  - **Sécurité** : paramètre de sécurité pour SSID 3.
- **SSID 4** : nom public du quatrième réseau sans fil.
  - **Sécurité** : paramètre de sécurité pour SSID 4.

État des paramètres de pare-feu

- **DoS (Déni de service)** : indique si la prévention DoS est active ou non.
- **Bloquer la requête de WAN** : indique si le blocage de la requête WAN est actif ou non.
- **Gestion à distance** : indique si la gestion à distance est active ou non (par exemple, si le gestionnaire de dispositifs du Cisco RV110W est accessible à distance).

État des paramètres VPN

- **Connexions QuickVPN disponibles** : nombre de connexions QuickVPN disponibles.
- **Connexions VPN PPTP disponibles** : nombre de connexions VPN PPTP disponibles.
- **Utilisateurs QuickVPN connectés** : nombre d'utilisateurs QuickVPN connectés.
- **Utilisateurs VPN PPTP connectés** : nombre d'utilisateurs VPN PPTP connectés.

Affichage des statistiques relatives au réseau sans fil

La page **Statistiques sans fil** affiche le cumul des statistiques sans fil pour la radio sur le périphérique.

Pour afficher les statistiques sans fil :

ÉTAPE 1 Sélectionnez **État** > **Statistiques sans fil**.

ÉTAPE 2 Dans le menu déroulant **Taux d'actualisation**, sélectionnez une fréquence d'actualisation.

ÉTAPE 3 (Facultatif) Par défaut, les données d'octets sont affichées en octets et les autres données numériques sont exprimées sous forme développée. Pour afficher les octets en kilo-octets (Ko) et les données numériques sous forme d'arrondi, cochez la case **Afficher les données statistiques simplifiées** et cliquez sur **Enregistrer**.

ÉTAPE 4 Pour réinitialiser les compteurs de statistiques sans fil, cliquez sur **Réinitialiser les compteurs**.

La page **Statistiques sans fil** affiche les informations suivantes :

Nom SSID	Le nom du réseau sans fil.
Paquet	Le nombre de paquets sans fil reçus/envoyés signalés à la radio sur tous les SSID configurés et actifs.
Octet	Nombre d'octets d'informations reçus/envoyés signalés à la radio sur tous les SSID configurés.
Erreurs	Nombre d'erreurs de paquets reçus/envoyés signalées à la radio sur tous les SSID configurés.
Abandonné	Nombre de paquets reçus/envoyés abandonnés par la radio sur tous les SSID configurés.
Multidiffusion	Le nombre de paquets en multidiffusion envoyés sur cette radio.
Collisions	Nombre de collisions de paquets signalées au routeur.

REMARQUE Les compteurs sont réinitialisés au redémarrage de l'appareil.

Affichage de l'état du VPN

La page **VPN** affiche l'état des connexions VPN.

Pour voir l'état de connexion des utilisateurs VPN, sélectionnez **État** > **État du VPN**.

La page **VPN** affiche les informations suivantes :

Nom d'utilisateur	Nom de l'utilisateur VPN associé au tunnel PPTP ou QuickVPN.
IP distante	Affiche l'adresse IP du client QuickVPN distant. Il peut s'agir d'une IP NAT/publique si le client se trouve derrière le routeur NAT.
État	Affiche l'état actuel du client QuickVPN. HORS LIGNE signifie que le tunnel QuickVPN n'est pas initié/établi par l'utilisateur VPN. EN LIGNE signifie que le tunnel QuickVPN, initié/établi par l'utilisateur VPN, est actif.
Heure de début	Heure à laquelle l'utilisateur VPN établit une connexion.
Heure de fin	Heure à laquelle l'utilisateur VPN met fin à une connexion.
Durée (secondes)	Durée entre l'établissement et la fin d'une connexion par l'utilisateur VPN.
Protocole	Protocole sélectionné par l'utilisateur : QuickVPN ou PPTP.

Vous pouvez modifier l'état d'une connexion pour établir ou déconnecter le client VPN configuré.

Pour mettre fin à une connexion VPN active, cliquez sur **Déconnexion**.

Affichage de l'état des connexions IPsec

L'état des connexions IPSec indique l'état des stratégies VPN actives sur le Cisco RV110W. (Ces stratégies sont configurées sur la page **VPN** > **Configuration VPN avancée**.) Pour afficher l'état des connexions IPSec :

ÉTAPE 1 Sélectionnez **État** > **État de la connexion IPSec**.

ÉTAPE 2 La table contient les informations suivantes :

- **Fréquence d'actualisation** : choisissez la fréquence à laquelle vous souhaitez que l'affichage des données soit actualisé.
- **Afficher les données statistiques simplifiées** : par défaut, les données d'octets sont affichées en octets et les autres données numériques sont exprimées sous forme développée. Pour afficher les octets en kilo-octets (Ko) et les données numériques sous forme d'arrondi, cochez la case **Afficher les données statistiques simplifiées**.
- **Nom de la stratégie** : nom de la stratégie VPN pour laquelle les données sont affichées.
- **Locale** ou **Distante** : affiche les adresses IP locale et distante.
- **Heure de début** et **Heure de fin** : affiche les heures de début et de fin des connexions IPSec.
- **Durée** : indique la durée d'activation de la connexion.
- **Paquet** : affiche les paquets reçus (Rx) et transmis (Tx) sur la connexion.
- **Octet** : affiche les octets reçus (Rx) et transmis (Tx) sur la connexion.
- **État** : affiche l'état de la connexion (par exemple, active ou non connectée).
- **Action** : affiche les actions que vous pouvez effectuer sur la connexion (par exemple, déconnecter).

ÉTAPE 3 Si vous avez effectué des modifications, cliquez sur **Enregistrer**.

Affichage des journaux

La page **Afficher les journaux** permet de consulter les journaux du Cisco RV110W.

Pour afficher les journaux :

ÉTAPE 1 Sélectionnez **État** > **Afficher les journaux**.

ÉTAPE 2 Cliquez sur **Actualiser les journaux** pour afficher les entrées de journal les plus récentes.

ÉTAPE 3 Pour filtrer les journaux ou spécifier la sévérité des journaux à afficher, cochez les cases en regard du type de journal correspondant et cliquez sur **OK**. Notez que tous les types de journaux au-delà d'un type sélectionné sont automatiquement inclus et qu'il n'est pas possible de les désélectionner. Par exemple, choisir des journaux « erreur » entraîne la sélection des journaux critiques, d'urgence et d'alerte, en plus des journaux d'erreur.

Les niveaux de sévérité des événements sont répertoriés du niveau le plus élevé au plus faible, comme suit :

- **Urgence** : le système n'est pas utilisable.
- **Alerte** : une action est requise.
- **Critique** : le système est dans un état critique.
- **Erreur** : le système subit une condition d'erreur.
- **Avertissement** : un avertissement système a été généré.
- **Notification** : le système fonctionne correctement, mais une notification système a été générée.
- **Information** : informations du périphérique.
- **Débogage** : fournit des informations détaillées sur un événement.

Pour supprimer toutes les entrées de la fenêtre des journaux, cliquez sur **Effacer les journaux**.

Pour enregistrer tous les messages de journal du pare-feu sur le disque dur local, cliquez sur **Enregistrer les journaux**.

Pour spécifier le nombre d'entrées à afficher par page, sélectionnez un nombre dans le menu déroulant.

Utilisez les boutons de navigation pour parcourir les pages des journaux.

Affichage des périphériques connectés

La page **Appareils connectés** affiche des informations sur les périphériques actifs connectés au Cisco RV110W.

La table ARP IPv4 affiche des informations émanant de périphériques qui ont répondu à la demande ARP (Address Resolution Protocol, protocole de résolution d'adresse) du Cisco RV110W. Si un périphérique ne répond pas à la demande, il est supprimé de la liste.

La table NDP IPv6 affiche tous les périphériques NDP (Neighbor Discover Protocol) IPv6 connectés à la liaison locale du Cisco RV110W.

Pour afficher les périphériques connectés :

ÉTAPE 1 Sélectionnez **État** > **Appareils connectés**.

ÉTAPE 2 Dans la table ARP IPv4, vous pouvez spécifier les types des interfaces à afficher. Il vous suffit pour cela de sélectionner une option dans le menu déroulant **Filtre**. Sélectionnez l'une des options suivantes :

Tous	Affiche une liste de tous les périphériques connectés au routeur.
Voyant WIRELESS	Affiche une liste de tous les périphériques connectés via l'interface sans fil.
Filaire	Affiche une liste de tous les périphériques connectés via les ports Ethernet sur le routeur.
WDS	Affiche une liste de tous les périphériques WDS (système de distribution sans fil) connectés au routeur.

Affichage des statistiques des ports

La page **Statistiques des ports** affiche les statistiques des ports.

Pour afficher les statistiques des ports :

ÉTAPE 1 Choisissez **État** > **Statistiques des ports**.

ÉTAPE 2 Dans le menu déroulant **Taux d'actualisation**, sélectionnez une fréquence d'actualisation. La page lit une nouvelle fois les statistiques depuis le routeur et s'actualise.

ÉTAPE 3 (Facultatif) Par défaut, les données d'octets sont affichées en octets et les autres données numériques sont exprimées sous forme développée. Pour afficher les octets en kilo-octets (Ko) et les données numériques sous forme d'arrondi, cochez la case **Afficher les données statistiques simplifiées** et cliquez sur **Enregistrer**.

ÉTAPE 4 Pour réinitialiser les compteurs de statistiques des ports, cliquez sur **Réinitialiser les compteurs**.

Cette table affiche les statistiques de transfert de données des ports WAN, LAN et VLAN dédiés, y compris la durée pendant laquelle ils ont été activés.

La page **Statistiques des ports** affiche les informations suivantes :

Interface	Le nom de l'interface réseau.
Paquet	Le nombre de paquets reçus/envoyés.
Octet	Nombre d'octets d'informations reçus/envoyés par seconde.
Erreurs	Le nombre d'erreurs de paquets reçus/envoyés.
Abandonné	Le nombre de paquets reçus/envoyés abandonnés.
Multidiffusion	Le nombre de paquets en multidiffusion envoyés sur cette radio.
Collisions	Le nombre de collisions de signal survenues sur ce port. Une collision survient lorsque le port essaie d'envoyer des données en même temps qu'un port sur un autre routeur ou ordinateur connecté à ce port.

Affichage de l'état du réseau invité

Les statistiques du réseau invité fournissent des informations sur le réseau invité sans fil configuré sur le Cisco RV110W. Pour voir l'état du réseau invité, sélectionnez **État** > **État du réseau invité**. Les informations suivantes sont indiquées :

- **Nom d'hôte** : périphérique connecté au réseau invité.
- **Adresse IP** : adresse IP attribuée au périphérique connecté.
- **Adresse MAC** : adresse MAC ou matérielle du périphérique connecté.
- **Temps restant** : temps de connexion restant du périphérique au réseau invité. (Les limites de temps sont configurées dans la page **Sans fil** > **Paramètres de base** > **Paramètres du réseau invité**.)
- **Action** : actions que vous pouvez effectuer sur le périphérique connecté (par exemple, déconnecter).

A

Utilisation de Cisco QuickVPN

Présentation

Cette annexe explique comment installer et utiliser le logiciel Cisco QuickVPN, disponible en téléchargement depuis Cisco.com. QuickVPN est compatible avec les ordinateurs fonctionnant sous Windows 7, Windows XP, Windows Vista ou Windows 2000 (les ordinateurs fonctionnant avec d'autres systèmes d'exploitation devront utiliser un logiciel VPN tiers).

Cette annexe comprend les sections suivantes :

- **Avant de commencer**
- **Installation du logiciel Cisco QuickVPN**
- **Utilisation du logiciel Cisco QuickVPN**

Avant de commencer

Le programme QuickVPN fonctionne uniquement avec un routeur correctement configuré pour accepter une connexion QuickVPN. Procédez comme suit :

ÉTAPE 1 Activez la gestion à distance. Reportez-vous à la section **Configuration des paramètres de base du pare-feu**.

ÉTAPE 2 Créez des comptes d'utilisateur QuickVPN. Reportez-vous à la section **Configuration du protocole PPTP**. Une fois le compte d'utilisateur créé, les informations de connexion peuvent être utilisées par le client QuickVPN.

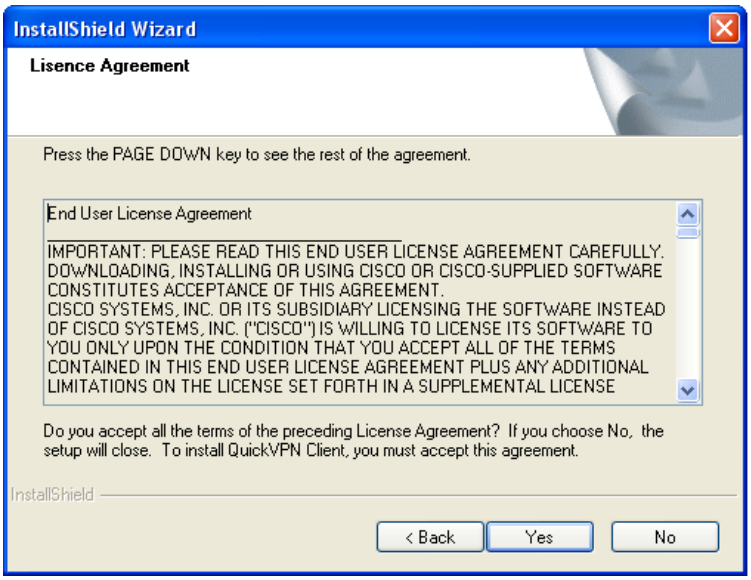
Installation du logiciel Cisco QuickVPN

Installation à partir du CD-ROM

ÉTAPE 1 Insérez le CD-ROM du Cisco RV110W dans le lecteur de CD-ROM. Lorsque l'assistant de configuration démarre, cliquez sur le lien **Install QuickVPN** (installer QuickVPN).

La fenêtre License Agreement (contrat de licence) s'affiche.

Contrat de licence


InstallShield Wizard
Lisence Agreement
Press the PAGE DOWN key to see the rest of the agreement.
End User License Agreement
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.
CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE ITS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE
Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install QuickVPN Client, you must accept this agreement.
InstallShield
< Back
Yes
No
193877

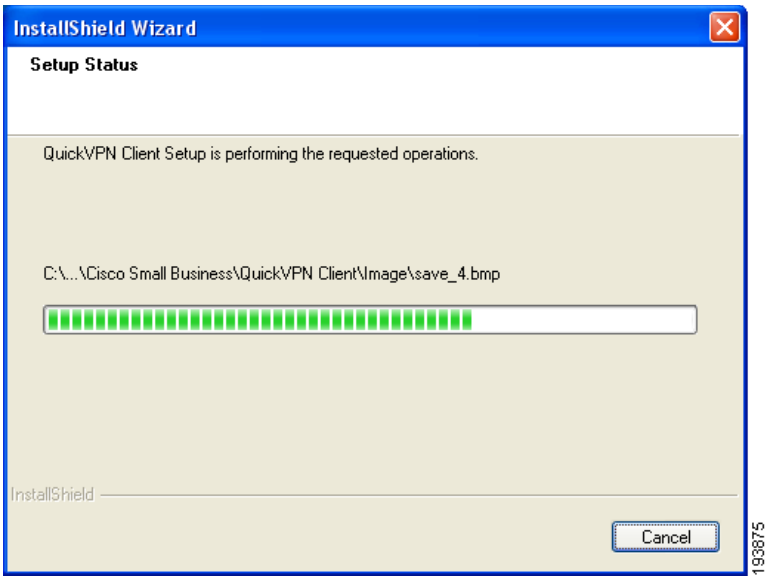
ÉTAPE 2 Cliquez sur **Yes** (oui) pour accepter le contrat.

ÉTAPE 3 Cliquez sur **Parcourir** et choisissez la destination de copie des fichiers (par exemple, C:\Cisco Small Business\QuickVPN Client).

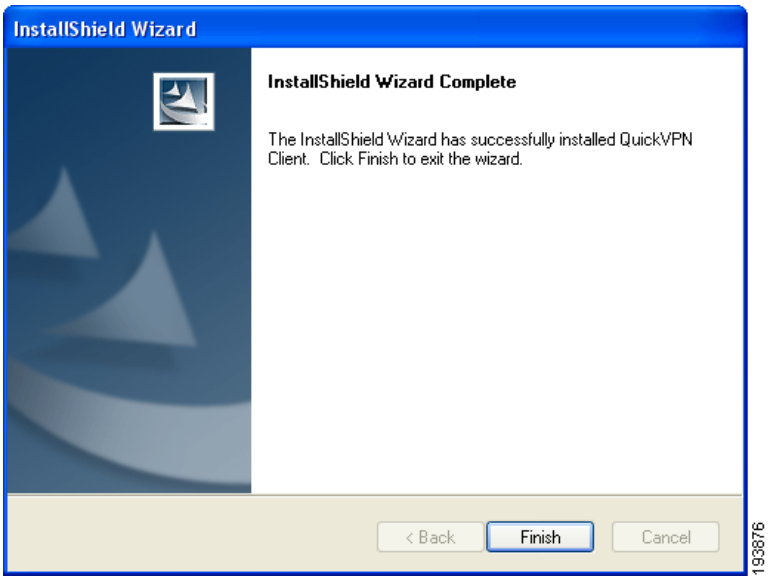
ÉTAPE 4 Cliquez sur **Next** (suivant).

L'assistant de configuration copie les fichiers vers l'emplacement sélectionné.

Copie des fichiers



Installation des fichiers terminée



ÉTAPE 5 Cliquez sur **Finish** (terminer) pour terminer l'installation. Passez à la section **« Utilisation du logiciel Cisco QuickVPN », page 158**.

Téléchargement et installation à partir d'Internet

ÉTAPE 1 Consultez la section Téléchargements de logiciel à l'**Annexe B, « Pour en savoir plus »**.

ÉTAPE 2 Saisissez Cisco RV110W dans la zone de recherche et recherchez le logiciel **QuickVPN**.

ÉTAPE 3 Enregistrez le fichier .zip sur votre ordinateur avant d'extraire le fichier .exe.

ÉTAPE 4 Double-cliquez sur le fichier .exe, puis suivez les instructions affichées à l'écran.

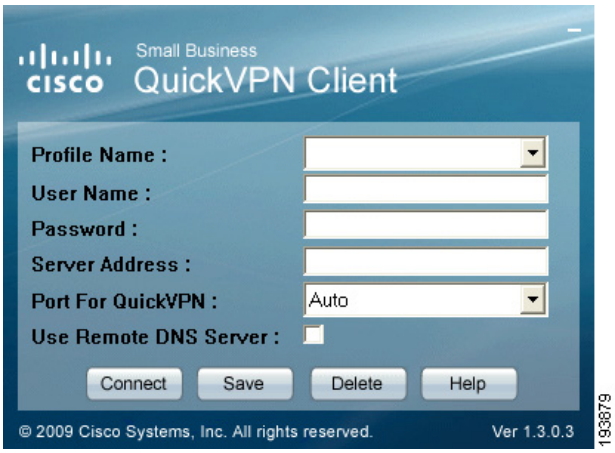
Utilisation du logiciel Cisco QuickVPN

ÉTAPE 1 Double-cliquez sur l'icône Cisco QuickVPN située sur le bureau ou dans la barre d'état système.

QuickVPN Desktop Icon

QuickVPN Tray Icon—
No Connection

La fenêtre QuickVPN Login (connexion à QuickVPN) s'affiche.



ÉTAPE 2 Dans le champ **Profile Name** (nom de profil), saisissez le nom à attribuer à votre profil.

ÉTAPE 3 Dans les champs **User Name** (nom d'utilisateur) et **Password** (mot de passe), saisissez le nom d'utilisateur et le mot de passe créés à la section **Création et gestion des utilisateurs QuickVPN**.

ÉTAPE 4 Dans le champ **Server Address** (adresse de serveur), saisissez l'adresse IP ou le nom de domaine du Cisco RV110W.

ÉTAPE 5 Dans le champ **Port For QuickVPN** (port pour QuickVPN), saisissez le numéro de port qu'utilise le client QuickVPN pour communiquer avec le routeur VPN distant ou laissez le paramètre par défaut, **Auto** (automatique).

ÉTAPE 6 Pour enregistrer ce profil, cliquez sur **Save** (enregistrer).

Pour supprimer ce profil, cliquez sur **Delete** (supprimer). Pour obtenir plus d'informations, cliquez sur **Help** (aide).

REMARQUE Si vous êtes amené à créer des tunnels vers plusieurs sites, vous pouvez créer plusieurs profils, mais un seul tunnel pourra être actif à la fois.

ÉTAPE 7 Pour lancer la connexion QuickVPN, cliquez sur **Connect** (se connecter).

L'évolution de la connexion s'affiche : *Connecting* (connexion), *Provisioning* (mise en service), *Activating Policy* (activation de la stratégie) et *Verifying Network* (vérification du réseau).

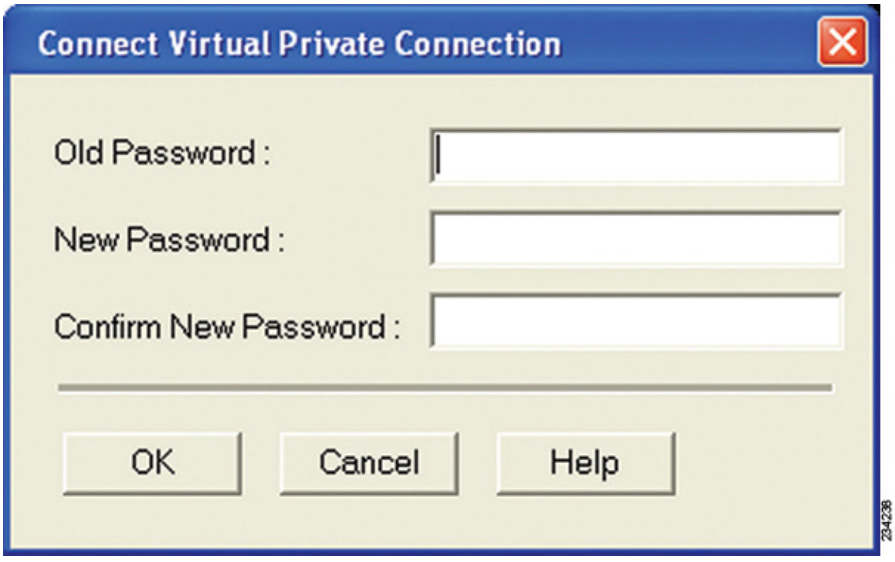
ÉTAPE 8 Une fois la connexion QuickVPN établie, l'icône QuickVPN dans la barre des tâches devient verte et la fenêtre QuickVPN Status (état QuickVPN) s'affiche.

La fenêtre affiche l'adresse IP de l'extrémité distante du tunnel VPN, la date et l'heure d'ouverture du tunnel VPN et la durée totale d'activité du tunnel VPN.

QuickVPN Tray Icon—Connection

Pour désactiver le tunnel VPN, cliquez sur **Disconnect** (déconnecter). Pour modifier le mot de passe, cliquez sur **Change Password** (modifier le mot de passe). Pour obtenir plus d'informations, cliquez sur **Help** (aide).

ÉTAPE 9 Si vous avez cliqué sur **Change Password** (modifier le mot de passe) et que vous êtes autorisé à modifier votre propre mot de passe, la fenêtre **Connect Virtual Private Connection** (connexion privée virtuelle) s'affiche.



ÉTAPE 10 Saisissez votre mot de passe dans le champ **Old Password** (ancien mot de passe). Saisissez votre nouveau mot de passe dans le champ **New Password** (nouveau mot de passe). Saisissez-le à nouveau dans le champ **Confirm New Password** (confirmer le nouveau mot de passe).

ÉTAPE 11 Cliquez sur **OK** pour enregistrer votre nouveau mot de passe.

REMARQUE Vous pouvez modifier votre mot de passe uniquement si la case **Allow User to Change Password** (autoriser l'utilisateur à modifier le mot de passe) a été cochée pour votre nom d'utilisateur. Reportez-vous à la section **Création et gestion des utilisateurs QuickVPN**.

B

Pour en savoir plus

Cisco propose de nombreuses ressources pour vous aider à tirer le meilleur parti du Cisco RV110W.

Ressources sur les produits

Assistance	
Communauté d'assistance Cisco Small Business	www.cisco.com/go/smallbizsupport
Assistance et documentation technique en ligne (Identification obligatoire)	www.cisco.com/support
Coordonnées de l'assistance téléphonique	www.cisco.com/en/US/support/tsd_cisco_small_ business_support_ center_contacts.html
Téléchargements de logiciel (Identification obligatoire)	Rendez-vous sur le site tools.cisco.com/support/downloads, puis saisissez le numéro du modèle dans la zone de recherche de logiciels Software Download Search.
Documentation sur les produits	
Cisco RV110W	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html
Cisco Small Business	
Site Cisco Partner Central pour les petites entreprises (connexion partenaire requise)	www.Cisco.com/web/partners/sell/smb
Accueil Cisco Small Business	www.Cisco.com/smb
Marketplace	www.cisco.com/go/marketplace